Vermoedens in de wiskunde, fascinerende vooruitgang.

Frans Oort

2009

HOVO-cursus wiskunde
Utrecht, maart/april 2009

Inhoudsopgave.

Inleiding

Zo vaak zeggen mijn vrienden en kennissen dat ze graag wat meer over wiskunde willen weten en horen. Maar hoe kan ik dat doen op een bevattelijke manier zonder de waarheid geweld aan te doen? Al werkend aan deze cursus merk ik dat er inderdaad veel is wat op een begrijpelijk niveau de fascinerende schoonheid van wiskunde kan laten zien.

"Wat me trof in al mijn gesprekken met hen was de buitengewone nauwkeurigheid waarmee ze zich uitdrukten ... de precieze opbouw van het antwoord ... dat wiskundigen domweg een hekel hebben aan het doen van een onware uitspraak ... " Zie de Nederlandse versie van [86], pagina 12.

Iets uitleggen wil ik doen op een wiskundig juiste manier. Zo vaak wordt er in onze wereld populariserend geschreven en gesproken (daar heb ik niets op tegen). Maar de grens wordt overschreden als we daarbij onware uitspraken doen. En dit gehoor zal dat ongetwijfeld als storend ervaren.

In deze syllabus, en in mijn cursus probeer ik onderwerpen te behandelen die zonder voorkennis begrepen kunnen worden. En er blijkt veel moois te doen te zijn. Op en avond vroegen twee nichtjes van me, die geen exacte opleiding/achtergrond hebben, of ik iets kon laten zien van wat wiskundigen zo fascineert. Ik liet ze een mooie puzzel en het wiskundige mechanisme daarachter zien. Ze begrepen een (tamelijk moeilijk) wiskundig bewijs. Het bevestigde mijn verwachting dat dit materiaal kan worden uitgelegd aan iedereen die bereid is na te denken, ongeacht de voorkennis.

In deze cursus probeer ik te laten zien hoe een moderne wiskundige werkt. Een van de aspecten daarvan is de volgende ontwikkeling die we vaak zien in wiskundige onderzoek:

we bestuderen een probleem, vaak is nieuwsgierigheid de directe aanleiding (zou dit zó of zó in elkaar zitten?);

voorbeelden, berekeningen, theorie, de wiskundige probeert voeling te krijgen met het materiaal;

de intuïtie zegt: alles wijst op een simpele en elegante oplossing; de formulering daarvan noemen we soms een *vermoeden*;

het kan dat dat vermoeden lang open blijft (we zullen er veel voorbeelden van zien);

maar het gebeurt ook wel dat de oplossing in een heel ander deel van de wiskunde blijkt te liggen (we hadden kennelijk nog niet begrepen wat de essentie van het probleem was).

Open vragen, vermoedens geven vaak richting in onderzoek; soms wordt een heel nieuw vakgebied ontwikkeld om dat probleem op te lossen; soms blijft het probleem eeuwen lang open, een uitdaging voor wiskundigen.
Ook blijkt: naarmate we meer weten wordt het aantal open problemen ook groter. Wiskunde is niet allen fascinerend, maar ook springlevend.

We volgen onder andere de lijn:

welke regelmatige veelhoeken zijn te construeren met passer en lineaal? (Een probleem uit de oude Griekse wiskunde.)

Gauss geeft op heel jonge leeftijd een oplossing.

Maar dan blijkt al snel dat hiermee het probleem verschoven is naar de vraag welke "'Fermat getallen" een priemgetal zijn; tot op heden onopgelost (ondanks veel theorie en berkeningen op grote computers);

we hebben geen idee hoe we die vraag bevredigend kunnen beantwoorden.

Of: een probleem uit de oude Griekse wiskunde is dat van de "perfecte getallen".
Gedeeltelijk opgelost, in de zin dat we weten hoe we die moeten zoeken (dat wist Euclides al).
Maar een uiteindelijk antwoord weten we pas als we weten welke Mersenne getallen een priemgetal zijn. Ondanks heel veel werk nog steeds niet bevredigend opgelost.

Een suggestie/verzoek van mijn kant.
(1) Als U iets niet begrijpt in mijn uitleg, *stel dan direct een vraag.* Graag wil ik U veel mooie dingen laten zien. Maar dat kan alleen maar als U het ook kunt volgen.
(2) Probeer elke keer *een bewijs zelf uit te schrijven.* Probeer ook elke keer een vraagstuk of een opgave zelf op te lossen. Het blijkt dat men weinig pleizier beleeft in het algemeen aan "alleen maar luisteren", maar juist veel pleizier beleeft als men actief de geboden stof volgt, zelf dingen uitzoekt, nieuwsgierig blijft, bij elk nieuw onderwerp zich afvraagt hoe iets in elkaar zou zitten.
(3) Elke keer zal ik ook een onderwerp of een puzzel behandelen die nu niet direct met de stof te maken heeft. Als U af en toe de algemene lijn te abstract vindt, dan is misschien dat onderdeel van het college stimulerend, geeft U wellicht een tevreden gevoel daar genoegen aan beleefd te hebben.
(4) Wat ik hoop en verwacht U te laten zien: een probleem lijkt moeilijk, maar als je ziet wat de wiskundige theorie er achter is, *dan is het probleem eenvoudig, elegant en prachtig.* In § 11 zien we daar een mooi, elementair voorbeeld van. Ik hoop dat U dat ook ervaart in allerlei meer gecompliceerde problemen.
(5) *Bewijsmethoden zijn essentiëel in de wiskunde.* Vaak kunt je over oneindig veel verschillende gevallen iets zeggen met één eenvoudige redenering.

We zullen zien: een bewijs uit het ongerijmde (neem aan dat iets niet waar, kom tot een tegenspraak, conclusie: het is wel waar).

We zullen ook zien: een bewijs met volledige inductie (voor elke $i \geq 0$ is er een uitspraak $U(i)$ gegeven; bewijs dat $U(1)$ waar is; neem aan, inductie-aanname, dat uitspraak $U(n)$ waar is voor $n \geq 1$; bewijs, inductie-stap, dat dan volgt dat $U(n+1)$ waar is; conclusie: $U(i)$ is waar voor alle $i \geq 1$); één stap bewijst oneindig veel gevallen.

Ik hoop dat U kunt genieten van de schoonheid van zulke bewijzen.

"Elke formule in een tekst halveert het aantal geïnteresseerde lezers.
Als dit zo zou zijn dan heeft deze syllabus aan het eind bar weinig lezers over. Mooie wiskunde kun je nu eenmaal niet uitleggen zonder logische stappen te beschrijven met wiskundige terminologie, zonder de gedachten te preciseren in compacte formules. In vroegere wiskundige culturen werd soms wiskunde beschreven in lange teksten, die bovendien niet precies genoeg waren. In de moderne wiskunde kunnen we een hoge mate van precisie bereiken door de dingen die we beschrijven met eenvoudige en directe definities te omschrijven, en vervolgens met duidelijke formules de voortgang van de ge-

dachtengang te ondersteunen. – Ja, dat kan wel eens abstract worden. Daarom is het zo goed als een wiskundige tekst gelardeerd wordt met uitleg, voorbeelden en berekeningen, beschrijven van de achtergrond, benoemen van de wiskundige intuïtie, en vooral door het expliciet maken van "dwarsverbanden" (bij voorbeeld een algebraïsche formule meetkundig begrijpen, we zullen daar mooie voorbeelden van zien).

Hier en daar zal ik wat verder gaan dan elementaire voorkennis toestaat. Elk onderdeel waar iets meer voorkennis verondersteld wordt wordt met een * aangegeven. Zulke onderdelen kunt U gerust overslaan. *Al het andere materiaal hoop ik, verwacht ik, is geheel toegankelijk voor iedereen die durft na te denken, die bereid is abstracte gedachten toe te laten.*

De schoonheid van wiskunde bestaat eigenlijk uit twee totaal verschillende componenten.

Een ervan is die ongebreidelde stroom van nieuwe gedachten, vergezichten in een abstracte wereld, het plotseling eenvoudig worden van een probleem dat eerst onoplosbaar en erg moeilijk leek. Over de intuïtie van de wiskundige die hieraan ten grondslag ligt zal ik in de cursus af en toe komen te spreken.

Een ander aspect is het feit dat je al die vergezichten, die prachtige gedachten kunt vatten in precieze beschrijvingen, kunt bewijzen in sluitende gedachtengangen. – Ik hoop en verwacht van alle deelnemers dat hier aan de slag gaan: niet alleen passief luisteren, maar ook vragen stellen, en vooral elke week tenminste één bewijs zelfstandig en volledig uitschrijven. Zo krijgt U voeling met deze wondere wereld, zo ziet U hoe een beetje nadenken inzicht kan geven.

In de cursus zal ik wiskundige notatie gebruiken. Mogelijk heeft U even nodig om daar aan te wennen. Stel een vraag zodra U niet begrijpt wat ik opschrijf of zeg!

Aspecten uit de geschiedenis van de wiskunde kun je op twee wezenlijk verschillende manieren beschrijven. Enerzijds kan men kiezen voor de methode de notatie, het gedachten goed, de gevoelens van de periode die je beschrijft zorgvuldig te beschrijven in de taal en notatie van die tijd; een historicus zal in het algemeen deze weg volgen. Anderzijds kun je het historisch materiaal in moderne notatie en interpretatie weergeven. Hier heb ik voor voor deze tweede methode gekozen.

Een lijstje van een paar romans die wiskundigen beschrijven:

http://kasmana.people.cofc.edu/MATHFICT/mfview.php?callnumber=mf547

1 Priemgetallen

We beginnen met een heel klassiek onderwerp: priemgetallen. In deze paragraaf leiden we eenvoudige eigenschappen af. Het merendeel van dit materiaal en de relevante verwijzingen is te vinden in [100], [65]. Zie ook [7], [**?**].

(1.1) Definitie. We werken in de verzameling $\mathbb{Z}$ van alle gehele getallen. De notatie $d \mid a$ wordt gebruikt voor: d deelt a; dat wil zeggen, er betaat een $b \in \mathbb{Z}$ met $d{\cdot}b = a$. Een getal $p \in \mathbb{Z}_{>1}$ heet een priemgetal als 1 en p de enige positieve delers van p zijn:

$$d \in \mathbb{Z}_{>1}, \quad d \mid p \quad \Longrightarrow \quad d = p.$$

(1.2) Opmerking. Elk getal $a \in \mathbb{Z}_{>1}$ is deelbaar door een priemgetal.
Bewijs. Merk op dat de bewering juist is voor $a = 2$. Neem aan dat de bewering juist is voor alle a' met $1 < a' < a$ (inductie-aanname). Als a een priemgetal is dan zijn we klaar. Als A niet een priemgetal is, dan heeft a een deler d heeft met $1 < d < a$. Schrijf $a = d{\cdot}a'$. De inductie veronderstelling bewijst dat er een priemgetal p is dat a' deelt. Dan is p ook een deler van a. QED

(1.3) Stelling. *Voor elk getal $a \in \mathbb{Z}_{>1}$ is er een ontbinding $a = p_1 \times \cdots \times p_t$ in priemfactoren. Een dergelijke ontbinding in priemfactoren is eenduidig op volgorde van de factoren na.*

Hiermee wordt bedoeld: voor elke $n \in \mathbb{Z}$ met $n \notin \{-1, 0, +1\}$ bestaan er priemgetallen $p_1, \cdots, p_s$ met $n = \pm p_1 \times \cdots \times p_s$. Bovendien als $p_1 \times \cdots \times p_s = \ell_1 \times \cdots \times \ell_t$ waar alle factoren priemgetallen zijn, dan is $s = t$ en na eventueel omnummeren geldt $p_1 = \ell_1, \ \cdots \ , p_s = \ell_s$.

We hoeven alleen maar factorizatie voor positieve gehele getallen te beschouwen. We kunnen (formeel) ook staande houden dat 1 een dergelijk factorizatie heeft, door te postuleren dat het lege product de waarde 1 heeft. We kunnen ook negatieve getallen in de beschouwingen betrekken; in dat geval moeten we de formulering wat aanpassen.

In § 16 ontwikkelen we een methode om dit te bewijzen, zie (16.3). We zullen deze stelling gebruiken, zonder verdere verwijzing.

(1.4) Voorbeelden. De getallen $2, 3, 5, \cdots$ zijn priemgetallen.

Zijn er veel priemgetallen? Waar liggen ze? Hoe vinden we priemgetallen? En, hoe kunnen we dit begrip gebruiken?
We beginnen met een stelling die al heel lang geleden bewezen werd:

(1.5) Stelling (Euclides, Boek IX, Prop. 20). *Er zijn oneindig veel priemgetallen.*
Bewijs. We zagen dat er tenminste één priemgetal is. (Bij voorbeeld 2.) Neem een

eindige, niet lege verzameling priemgetallen $\{p_1, p_2, \cdots, p_t\}$. We laten zien dat er nog een priemgetal is dat niet in deze verzameling ligt. Beschouw

$$a := p_1 \times p_2, \times \cdots \times p_t + 1.$$

Dit getal a is deelbaar door een priemgetal, zie (1.2); we schrijven p voor een van de priemgetallen die a deelt.
Bewering: $p \neq p_i$ voor alle $1 \leq i \leq t$.
Inderdaad, bij deling met rest van a door p_i is de rest 1. En bij deling met rest a door p is de rest 0. Hieruit volgt dat de bewering juist is.

Dit bewijst dat de verzameling van priemgetallen niet eindig is. QED

(1.6) Wat een schitterend bewijs. We willen laten zien dat iets niet eindig is. En dat doen we door één stap te bewijzen.
Oefenen in het noteren met wiskundige symbolen. De laatste stap in het bewijs schrijf ik uit zoals een wiskundige dat liever doet:

$$\left.\begin{array}{l} a \equiv 1 \pmod{p_i} \\ a \equiv 0 \pmod{p} \end{array}\right\} \Longrightarrow p_i \neq p.$$

Uitleg: $a \equiv b \pmod{c}$ betekent: c deelt $a - b$. Het symbool $\Longrightarrow$ staat voor een logische implicatie: wat er links van staat bewijst dat wat er rechts van staat juist is.

(1.7) We kunnen de methode van het bewijs ook gebruiken om een oneindige rij van onderling verschillende priemgetallen te construeren. “Elke keer kiezen we het kleinste priemgetal dat a deelt”: begin met $p_1 = 2$ en dan komt er:

$$p_2 = 3, \quad p_3 = 2 \times 3 + 1 = 7, \quad p_4 = 2 \times 3 \times 7 + 1 = 43,$$

$$p_5 = 13 \quad \text{want} \quad (2 \times 3 \times 7 \times 43 + 1 = 1807 = 13 \times 139), \cdots .$$

Het is niet duidelijk dat we zo ook alle priemgetallen krijgen. En het is ook niet zo dat ze in de goede volgorde staan.

(1.8) **Opgave.** Construeer een rij priemgetallen op de volgende manier: begin met $p_1 = 2$, dan $p_2 = p_1^2 + 1 = 5$, en inductief verder door: p_{t+1} is het kleinste priemgetal dat $p_1^2 \times \cdots \times p_t^2 + 1$ deelt. *Bewijs dat in deze rij priemgetallen het getal* 3 *niet voorkomt.*

(1.9) Nog een manier om te bewijzen dat er *oneindig veel priemgetallen bestaan.* Met dank overgenomen uit:

http://www.wiskundemeisjes.nl/20080725/priemformule/

Neem $a(1) = 7$ en neem voor $n \geq 2$

$$a(n) = a(n-1) + \text{ggd}(n, a(n-1)).$$

We vinden bij de eerste stap $a(2) = a(1) + \text{ggd}(2, 7) = 8$. De verschillen tussen twee opeenvolgende termen $a(n) - a(n-1)$ geven priemgetallen (en een heleboel enen).

De reeks a begint zo:

$$7, 8, 9, 10, 15, 18, 19, 20, 21, 22, 33, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 69, \cdots$$

en dit zijn de bijbehorende verschillen $a(n) - a(n-1)$

$$1, 1, 1, 5, 3, 1, 1, 1, 1, 11, 3, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 23.$$

Als we de enen overslaan, dan krijgen we de priemgetallen $5, 3, 11, 3$ en 23. Als je zo verder gaat, dan vinden we (zonder de dubbelen en de enen) meer priemgetallen

$$5, 3, 11, 23, 47, 101, 7, 13, 233, 467, 941, 1889, 3779, 7559, 15131, 53, 30323, \cdots .$$

Eric Rowland bewijst in het artikel [80] dat in deze reeks alleen enen en priemgetallen voorkomen.

(1.10) We nummeren alle priemgetallen naar klimmende grootte, $p_i < p_{i+1}$ voor alle i:

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5, \cdots,\ p_{20} = 71, \cdots,\ p_{300} = 1987, \cdots \ .$$

Dat die rij bestaat is duidelijk. Maar ik zie niet in hoe je een priemgetal met een groot index-cijfer kent zonder alle vorige priemgetallen in deze rij te bepalen.

We geven nu voorbeelden van vragen over priemgetallen, en de opgave aan U is om eerst eens in te voelen of deze vragen moeilijke of gemakkelijk te beantwoorden zijn.

(1.11) We schrijven

$$\Delta_i = p_{i+1} - p_i,$$

het "gat"tussen twee opeenvolgende priemgetallen op deze plaats.
Vraag 1. Komen er willekeurig grote gaten voor? Of is de lengte van de gaten begrensd? Hoe beantwoord je een dergelijke vraag zonder dat je alle priemgetallen kent?
Vraag 2. Komt het maar eindig vaak of eindig vaak voor dat $\Delta_i = 2$? We zeggen dat p, q een priem-tweeling is als dit priemgetallen zijn met $q - p = 2$. Onze vraag is dus: is het aantal priem-tweelingen eindig of oneindig? Voorbeelden: $\{3, 5\}$, $\{5, 7\}$, $\{11, 13\}$ etc. ? Zie (9.10), (9.11).

We zullen veel later een stelling behandelen die laat zien dat de priemgetallen "steeds schaarser". Dat geeft een antwoord op de eerste vraag, maar niet op de tweede vraag.

(1.12) Eerste verrassing: Stelling. *Voor elke $N \in \mathbb{Z}_{>0}$ is er een i met $\Delta_i > N$.* (Met andere woorden: de lengte van de gaten is niet begrensd.)
Bewijs. Voor een gegeven N beschouw het getal

$$L := 2 \times 3 \times 4 \times j \times \cdots \times (N + 1).$$

Dit getal wordt wel genoteerd als: $L = (N + 1)!$, spreek uit: "$N + 1$ - faculteit". Merk op dat de getallen

$$L + 2, \quad L + 3, \quad L + 4, \cdots, \quad L + N + 1$$

niet priem zijn; want: $L+2, \cdots, N+j, \cdots L+N+1$ is deelbaar door $2, \cdots, j, \cdots, N+1$. Noem p_i het grootste priemgetal dat kleiner is dan $L+2$; dan is p_{i+1} het kleinste priemgetal dat groter is dan $L+N+1$. We zien:

$$p_{i+1} - p_i = \Delta_j \geq (L+N+2) - (L-1) > N.$$

QED

(1.13) Tweede verrassing: een open probleem, een vermoeden. Er zijn heel veel priemtweelingen gevonden. Het aantal priemtweelingen onder de 10^8 is veel groter dan het aantal inwoners van de USA. We hebben vermoedens die ongeveer aangeven hoeveel priemtweelingen er zijn onder een gegeven grens.

In 2007 was er een priemtweeling bekend waar elk van de twee priemgetallen bestaat uit 58711 cijfers.

Meestal schrijven we

$\pi_2(n)$ voor het aantal priemtweelingen $(p, p+2)$met $p \leq n$. Een paar voorbeelden:

$$\pi_2(10^8) = 440,312$$

$$\pi - 2(10^{16}) = 10,304,195,697,298$$

Als U graag rekenen wilt: *Bewijs dat* $\pi_2(1000) = 35$.
Zie:

http://en.wikipedia.org/wiki/Twin_prime
http://mathworld.wolfram.com/TwinPrimes.html

Zie (9.10)

(1.14) Opgave. a) Bepaal alle priemgetallen p zodanig dat ook $p+2$ en ook $p+4$ priem zijn.
b) Zij $(p, q = p+2)$ een priemtweeling met $p > 3$. Bewijs dat er een getal $n \in \mathbb{Z}_{>0}$ is zodanig dat $p = 6n-1$, $q = 6n+1$. Bewijs: als voor een priemtweeling (p, q) met $p > 5$ dat getal n voldoet aan $n \equiv apmod10$ met $0 \leq a < 10$, dan is $a \in \{0, 2, 3, 5, 7, 8\}$. Bewijs dat al deze waarden voor a voorkomen voor een priemtweeling.

(1.15) *Is er een formule die precies alle priemgetalen geeft*? We zullen zien dat dit te vaag geformuleerd is, dat er vele antwoorden zijn, maar dat het nut van die antwoorden beperkt is. Voor een overzicht en verwijzingen, zie [21], [22].

(1.16) Verrassende stelling. *Er is een getal $\alpha \in \mathbb{R}$ zodanig dat het n-de priemgetal gegeven wordt door:*

$$p_n \quad = \quad [10^{n(n+1)/2)} \cdot \alpha] - 10^n \cdot [10^{(n-1)n/2} \cdot \alpha].$$

Zie [62].
Uitleg: voor $x \in \mathbb{R}$ schrijven we $[x]$ voor het grootste gehele getal dat hoogstens x is (als $x \geq 0$: all cijfers achter de komma weglaten).

Dit lijkt toch prachtig: een formule die alle priemgetallen geeft. Maar het is mooier dan het lijkt. Een dergelijke α bestaat. Maar, om α te bepalen moeten we álle priemgetallen kennen, want

$$\alpha \quad = \quad \sum_{n=1}^{n=\infty} \frac{p_n}{10^{n(n+1)/2}} \quad = \quad 0.203005000700011000013\cdots \ .$$

Uitleg notatie:

$$\sum_{n=1}^{n=m} a_n \quad \text{betekent} \quad a_1 + a_2 + \cdots + a_m.$$

Om te bewijzen dat dit inderdaad werkt moeten we weten: $p_n < 10^n$. Is dit wel zo? Voor kleine priemgetallen is dit eenvoudig na te gaan. Maar verderop komen er soms veel grotere gaten. Hoe kunnen we dit bewijzen voor alle n ? Zie (6.21): als we (een zwakke vorm van) de priemgetalstelling hebben, dan kunnen we een dergelijk afschatting eenvoudig maken.

(1.17) Opgave. Definieer $\beta \in \mathbb{R}$ door:

$$p_n \quad = \quad [10^{n^2} \cdot \alpha] - 10^{2n-1} \cdot [10^{(n-1)^2} \cdot \alpha].$$

Geef een formule voor het n-de priemgetal p_n met behulp van β. Zie [22], pag. 20.

(1.18) Al leek het dan niet zo nuttig om "formules voor priemgetallen" vinden, er is wel een belangrijke bijdrage in deze richting. *Er is een polynoom* $P \in \mathbb{Z}[a, b, \cdots, x, y, z] = \mathbb{Z}[T_1, \cdots, T_{26}]$ *met gehele coëfficiënten van graad* 25 *in* 26 *variabelen, zodanig dat elke positieve waarde van dat polynoom* (substitueer gehele getallen voor de variabelen) *een priemgetal is, en zodanig dat alle priemgetallen op die manier verkregen worden* (J. P. Jones), zei [47], zie [19], pag.331; zie [22], pag. 21.

Dat heeft niet veel practisch nut (je moet heel veel rekenen om een priemgetal eruit te krijgen). Maar het is van groot technisch nut: dit lost een beroemd probleem uit de logica op. Zie [47], zie [19]. Zie ook [22].

(1.19) Deelbaarheid door 3. We laten zien dat het getal 1143123 niet een priemgetal is. Reken de som van de cijfers uit. Dat is gelijk aan 15 in dit geval. Omdat 15 deelbaar is door 3 volgt dat 1143123 deelbaar is door 3.
Bewijs: Als we 10 door 3 delen komt er rest 1. Algemener: als we 10^i met $i > 0$ door drie delen komt er rest 1. Daaruit volgt dat als we 1143123 door 3 delen er precies dezelfde rest komt als we $1 + 1 + 4 + 3 + 1 + 2 + 3$ door 3 delen.
Opgave. *Formuleer een criterium voor deelbaarheid door* 3 *en geef een bewijs.*
Opgave. *Formuleer een criterium voor deelbaarheid door* 9 *en geef een bewijs.*

(1.20) Deelbaarheid door 11. We laten zien dat 62135821 deelbaar is door 11. Merk op dat $6 + 1 + 5 + 2 = 2 + 3 + 8 + 1$ (de som van de cijfers met even rangnummer en van de cijfers met oneven rangnummer). Hieruit volgt dat 62135821 deelbaar is door 11.
Opgave. *Formuleer een criterium voor deelbaarheid door 11 en geef een bewijs.*

(1.21) Merk op: $7 \times 11 \times 13 = 1001$. Dit kunnen we gebruiken. Een voorbeeld: laat zien dat 58207897 niet deelbaar is door 7 en niet deelbaar is door 13. Is 800850052015 deelbaar door 13?

(1.22) **Opgave.** Een oude Chinese test of een gegeven getal priem is zegt:

$$(n \in \mathbb{Z}_{>1}, \quad n \mid (2^n - 2)) \quad \stackrel{?}{\Longrightarrow} \quad n \ \text{ is een priemgetal.}$$

Is dit juist?

(1.23) **Opgave.** Beschouw de veelterm $f = X^2 - X + 41$. Substitueer daarin de getallen $n = 0, 1, 2, \cdots$ etc. ? we zien steeds priemgetallen verschijnen (hoe lang gaan we door ?). *Is $f(n)$ een priemgetal voor elke $n \in \mathbb{Z}_{\geq 0}$?*

(1.24) Een oplossing van (1.8). Als 3 niet een deler is van een geheel getal n, dan is $n^2 \equiv 1 \pmod 3$. Dus is $p_1^2 \times \cdots \times p_t^2 + 1$ niet deelbaar door 3.

(1.25) Een oplossing van (1.14). a) Van de getallen $\{N, N+2, N+4\}$ is precies een deelbaar door 3. Als ze allemaal priem zijn dan is $N = 3$.
b) Als $a = 4$ of $a = 9$ dan is 5 een deler van $6N + 1$. Als $a = 1$ of $a = 6$ dan is 5 een deler van $6N - 1$.
Beschouw d en a voor: $p = 59$, $p = 11$, $p = 17$, $p = 29$, $p = 41$, $p = 107$.

(1.26) Een oplossing van (1.17)

$$p_n \quad = \quad [10^{n^2} \cdot \beta] - 10^{2n-1} \cdot [10^{(n-1)^2} \cdot \beta].$$

(1.27) Een oplossing van (1.22)*. Nee, dit is niet juist: neem $n = 341 = 11 \times 13$. Hoe laten we zien dat deze n aan de voorwaarde voldoet? Bedenk dat 2^{341} een getal van 103 cijfers is. We gaan het criterium niet decimaal berekenen. Daarom een bewijs waarin we wat techniek gebruiken.
Bedenk dat $(\mathbb{Z}/11)^*$ een (cyclische) groep is van orde 10. Dus is

$$(2 \bmod 11)^{341} = (2 \bmod 11)^{341-340}; \quad \text{dus} \quad 11 \mid (2^{341} - 2).$$

Uit $2^5 = 32$ bewijzen we:

$$(2 \bmod 31)^{341} = (2 \bmod 31)^{341-340}; \quad \text{dus} \quad 31 \mid (2^{341} - 2).$$

We concluderen dat $11 \times 13 \mid (2^{341} - 2)$. QED

Het getal 341 heet wel een "Carmichael getal" of een ""pseudo priemgetal".
Probeer ook eens 561.
Is het getal 1729 saai? Zie
http://www.mathpages.com/home/kmath028.htm
http://en.wikipedia.org/wiki/1729_(number)
Zie verder [7], § 8.

(1.28) Een oplossing van (1.23).
Stelling. (Euler) *$f(n)$ geeft een priemgetal geeft voor alle $0 \leq n \leq 40$.*
Maar hij wist natuurlijk best dat $f(41)$ *niet een priemgetal is.*

Vervang het getal 41 door een van de waarden $2, 3, 5, 11, 17$ en formuleer een analoge opgave/stelling.

2 Perfecte getallen

Hier is een klassiek probleem: *kennen we alle perfecte getallen?*

(2.1) Definitie. Een positief geheel getal $N > 1$ heet *perfect* als het de som is van de eigen echte positieve delers. (We zeggen dat d een echte deler is als d een deler is van N en als bovendien geldt $1 \leq d < N$.) Bij voorbeeld $6 = 1 + 2 + 3$ is een perfect getal.

We kunnen de definitie nog ander formuleren. Bij een gegeven $N \in \mathbb{Z}_{\geq 0}$ beschouwen we de getallen d die N delen met $1 \leq d \leq N$ (dus ook het getal $d = N$ zelf). We schrijven $\sigma(N)$ voor de som van deze delers. Herformulering: we zeggen dat N perfect is als $2N = \sigma(N)$.

Voorbeelden:

$$6 = 1 + 2 + 3, \quad \sigma(6) = 12; \quad 28 = 1 + 2 + 4 + 7 + 14, \quad \sigma(28) = 56.$$

Probeer zelf nog een perfect getal te vinden.

In de Griekse oudheid werden deze getallen bestudeerd en gedeeltelijk geclassificeerd.

Samenvatting. We schrijven

$$\sigma(N) := \sum_{1 \leq d \leq N,\ d \text{ deelt } N} d; \qquad N \text{ is perfect} \iff \sigma(N) = 2N.$$

Anders gezegd:

$$\sum_{1 \leq d < N,\ d \text{ deelt } N} d = N \iff N \text{ is perfect.}$$

(2.2) Definitie. Een geheel getal $p \geq 2$ heet een *priemgetal* als 1 en p de enige positieve delers van p zijn. M.a.w. als $1 < i < p$ dan is i niet een deler van p. We hebben dit reeds bestudeerd in § 1.

Voorbeelden: $2, 3, 5, 7, 11, 13, 17, \cdots$ zijn priemgetallen. Ga na dat 1143123 niet een priemgetal is. Ga na dat 62135821 niet een priemgetal is. (Als het niet lukt, kijk dan in §1).

Discussie. We noemen het getal 1 niet een priemgetal. Vroeger (b.v. in de tijd van Euler en Goldbach) was dat wel gebruikelijk. We komen hier nog op terug.

(2.3) Stelling (Euclides). *Een* even *getal N is een perfect getal is, dan en slechts dan als er een positief geheel getal $n \geq 2$ is zodanig dat:*

$$N = (2^n - 1)2^{n-1}, \quad \textit{en} \;\; M_n := 2^n - 1 \;\; \textit{is een priemgetal.}$$

(2.4) We laten we eerst een eenvoudig gedeelte van het bewijs zien. Neem aan dat $q := 2^n - 1 = M_n$ een priemgetal is. We zien dat echte delers van $N = (2^n - 1)2^{n-1} = (2^n - 1)\cdot q$ zijn:

$$1, 2, 4, \cdots, 2^{n-1}, \quad 1\cdot q, \quad 2\cdot q, \quad 4\cdot q, \quad \cdots, \quad (2^{n-2})\cdot q.$$

Daarom:

$$(1+2+4+\cdots+2^{n-1})+(1+2+4+\cdots+2^{n-2}){\cdot}q =$$
$$=(2^n-1)+(2^{n-1}-1){\cdot}(2^n-1)=2^{n-1}{\cdot}q=N.$$

Dit laat zien dat elk getal van de vorm $N=(2^n-1)2^{n-1}$, waar $M_n=2^n-1$ een priemgetal is, inderdaad een even perfect getal is.

We zien:

$$M_2=3,\quad (2^{2-1})M_2=6; \qquad M_3=7,\quad (2^{3-1})M_3=28.$$

We vinden direct al weer een nieuw even perfect getal:

$$M_5=31,\quad (2^{5-1})M_5=16\times 31=496.$$

Zoek zelf nog een ander perfect getal.

Vraag. *Kunnen we op deze manier alle (even) perfecte getallen vinden?*
Vraag. *Zijn er ook oneven perfecte getallen?*

(2.5) Definitie. Een getal van de vorm $M_n=2^n-1$ heet een *Mersenne getal*. Als bovendien M_n een priemgetal is, dan heet dit een *Mersenne priemgetal*.
Conclusie. *Er zijn even veel even perfecte getallen als Mersenne priemgetallen.*

(2.6) Lemma. *Voor $n>1$ geldt:*

$$M_n=2^n-1 \ \textit{ is een priemgetal} \quad\Longrightarrow\quad n \ \textit{ is een priemgetal.}$$

Bewijs. Als $n=s{\cdot}d$ met $s>1$ en $d>1$ dan geldt:

$$2^{sd}-1=(2^d-1)\left(2^{(s-1)d}+2^{(s-2)d}+\cdots+s^d+1\right) \quad \text{met}$$

$$(2^d-1)>1, \quad (2^{(s-1)d}+2^{(s-2)d}+\cdots+s^d+1)>1.$$

Dit laat zien: als n niet priem is, dan is M_n niet priem. Dit is hetzelfde als: als M_n priem is dan is n priem. QED

(2.7) Van de functie $\sigma()$ hierboven gedefiniëerd bewijzen we een eigenschap die we gaan gebruiken in een bewijs van (2.3).
Lemma. *Laat $a,b\in\mathbb{Z}_{>0}$ positieve gehele getallen zijn die onderling ondeelbaar zijn.* Daarmee bedoelen we: in de priemfactorontbinding van a komt geen deler van b voor; oftewel: $\mathrm{ggd}(a,b)=1$; zie (16.7). *Dan geldt:*

$$\sigma(ab)=\sigma(a)\sigma(b).$$

Bewijs. We gebruiken de eenduidigheid van de ontbinding in priemfactoren. Zie §16. Omdat $\mathrm{ggd}(a,b)=1$ is elke deler d van ab eenduidig van de vorm $d=a'b'$, waar a' een deler is van a en b' een deler van b. QED

We herschrijven met deze kennis het bewijs (2.4). Als $N = 2^{n-1}{\cdot}q$, waar $q = 2^n - 1$ een priemgetal is, dan geldt:

$$\sigma(N) \quad = \quad \sigma(2^{n-1})\sigma(q) \quad = \quad (2^n - 1)(1 + q) \quad = \quad 2N.$$

(2.8) Bewijs van (2.3). Rest ons nog te bewijzen:

N is even en perfect $\quad\Longrightarrow\quad N = (2^n - 1)2^{n-1}$, en $M_n := 2^n - 1$ is een priemgetal.

We schrijven $N = 2^{n-1}{\cdot}q$, met q oneven. Merk op dat $n > 1$ (omdat N even is). Dan geldt:

$$\sigma(N) \quad = \quad \sigma(2^{n-1}){\cdot}\sigma(q) \quad = \quad (2^n - 1){\cdot}\sigma(q) \quad = \quad 2^n{\cdot}q$$

(gebruik het voorgaande lemma, en gebruik dat N perfect is). Omdat $2^n - 1$ oneven is, volgt uit de laatste gelijkheid dat 2^n een deler is van $\sigma(q)$. Schrijf

$$\sigma(q) = 2^n{\cdot}A.$$

Merk op dat A een deler is van q met $1 \leq A < q$. Dan geldt:

$$(2^n - 1){\cdot}\sigma(q) = (2^n - 1){\cdot}2^n{\cdot}A = 2^n{\cdot}q; \quad \text{dus} \quad (2^n - 1){\cdot}A = q.$$

Dan is:

$$q + A = (2^n - 1){\cdot}A + A = 2^n{\cdot}A = \sigma(q).$$

Veronderstel $A > 1$; dan komt er een tegenspraak: in dat geval zijn 1, A en q delers van q, en we zouden krijgen $\sigma(q) \geq 1 + A + q$, een tegenspraak. We concluderen:

$$A = 1, \qquad q = 2^n - 1.$$

Uit

$$(2^n - 1){\cdot}\sigma(q) = 2^n{\cdot}q \quad \text{volgt dan} \quad \sigma(q) = 2^n.$$

Hieruit volgt dat 1 en $2^n - 1$ de enige delers zijn van $q = 2^n - 1$; dus is bovendien q een priemgetal. QED(2.3)

We zullen in de volgende paragraaf Mersenne priemgetallen bestuderen. Nu formuleren alvast het volgende

(2.9) Vermoeden.? *Er bestaan oneindig veel even perfecte getallen.*
We komen hier nog uitvoerig op terug.

(2.10) Opgave(Sylvester). *Stel dat een oneven getal n perfect is. Bewijs dat in dat geval n deelbaar is door ten minste* 3 *verschillende priemgetallen.*

(2.11) Bestaan er oneven perfecte getallen?
Rest ons nog de vraag of er *oneven perfecte getallen bestaan. Het antwoord op deze vraag is onbekend.*
Maar, ga niet zo maar zoeken, want we weten dat als er een oneven perfecte getal zou bestaan, dan is dat getal vreselijk groot. Zie:
http://mathworld.wolfram.com/OddPerfectNumber.html
In het bijzonder:

Brent et al (1991): Als N een oneven perfecte getal zou zijn, dan geldt: $N > 10^{300}$.

Hare (2005): Als N een oneven perfecte getal zou zijn,
dan heeft de factorontbinding van N tenminste 75 priemfactoren.

Discussie. Dit lijkt op "numerieke evidentie" voor het idee dat er misschien we helemaal geen oneven perfecte getallen bestaan. Kunnen we zo terecht een vermoeden formuleren? Ik kom hierop nog uitvoerig terug.

(2.12) Verwachting.? *Er bestaan geen oneven perfecte getallen.*

(2.13) Opgave(Sylvester). *Stel dat een oneven getal n perfect is. Bewijs dat in dat geval n deelbaar is door ten minste 3 verschillende priemgetallen.*

(2.14) Oplossing van Opgave (2.13). Laat zien dat p^α en $p^\alpha q^\beta$ niet perfect zijn voor priemgetallen $p < q$.

3 Mersenne priemgetallen

In de vorige paragraaf hebben we definitie van een Mersenne priemgetal gezien $M_n = 2_n - 1$, zodanig dat dit een priemgetal is, en het verband met even perfecte getallen. Kennen we alle Mersenne priemgetallen? Zo ja, dan zouden we ook alle even perfecte getallen kennen. We hebben ook in (2.6) gezien dat als M_n een priemgetal is, dan is n een priemgetal.

(3.1) Geldt de omkering van (2.6)? Of te wel; is het waar dat voor elk priemgetal p het Mersenne getal $M_p = 2^p - 1$ ook priem is? (Dat zou een gemakkelijke manier zijn om te laten zien (?) dat er oneindig veel Mersenne priemgetallen, en dus oneindig veel perfecte getallen zijn). Maar de vraag heeft een ontkennend antwoord:

$$M_{11} = 2^{11} - 1 = 2047 = 23 \times 89.$$

(3.2) **Stelling.** *Onderstel dat $q := 2n + 1$ een oneven priemgetal is. Dan is q óf een deler van $2^n - 1$ of een deler van $2^n - 1$.*
We zullen later in deze § een bewijs hiervan geven.

(3.3) **Opgave.** *We gaan na welk van de twee gevallen optreedt voor een paar kleine priemgetallen:*
17 deelt $2^8 - 1$,
3 deelt $2^1 + 1$,
5 deelt $2^2 + 1$,
7 deelt $2^3 - 1$.
Hoe gaat dit verder? Probeer regelmaat te ontdekken. Dit zouden we kunnen doen door een aantal voorbeelden door te rekenen. Kijk naar de gevallen in de tabel hieronder. Probeer te ontdekken wat voor soort regelmaat er in deze tabel zit. We schrijven $q = 2n + 1$; we weten dat q een deler is van $2^n + 1$ of van $2^n - 1$; en de tabel geeft voor elk priemgetal welke van de twee gevallen optreedt. Zien we hier twee gevallen van een priemgetal $n = p$ zodanig dat $2^p - 1$ niet een priemgetal is?

$q = 2n+1$	2^n	+/-
3	2	+
5	4	+
7	8	-
11	32	+
13	64	+
17	256	-
19	512	+
23	2048	-
29	16384	+
31	32768	-
37	262144	-
41	1048576	-
43	2097152	+
47	8388608	-
etc		

(3.4) Opmerking. Als $q = 2n + 1$ een oneven priemgetal is, dan is q een deler van $2^{2n-1} = (2^n + 1)(2^n - 1)$. Hier is het gegeven dat q een priemgetal is essentieel:

Beschouw $15 = 2{\cdot}7 + 1$. We zien: $2^7 + 1 = 127$ is priem en $2^7 - 1 = 125 = 5^3$. *Dus is* 15 *niet een deler van* $(2^7 + 1)(2^7 - 1)$.

(3.5) Hier is een lijst van de eerste 13 Mersenne priemgetallen en het grootste nu bekende. Hier is p een priemgetal en # staat voor het aantal cijfers van M_p. Voor deze informatie zie:

http://primes.utm.edu/mersenne/
http://mathworld.wolfram.com/MersennePrime.html

p	M_p	#	jaar	ontdekt door
2	3	1	oudheid	
3	7	1	oudheid	
5	31	2	oudheid	
7	127	3	oudheid	
13	8191	4	1461	Reguis, Cataldi(1603)
17	131071	6	1588	Cataldi
19	524287	6	1588	Cataldi
31	$\cdots$	10	1750	Euler
61	$\cdots$	19	1883	Pervouchine, Seelhoff(1886)
89	$\cdots$	27	1911	Powers
107	$\cdots$	33	1913	Powers
127	$\cdots$	39	1876	Lucas
521	$\cdots$	157	1952	Robinson
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
etc. ?				

Momenteel zijn er 46 Mersenne priemgetallen bekend (september 2008). Er werd en wordt ongelooflijk veel (reken)tijd aan besteed, vroeger door expliciete berekeningen, nu door een combinatie van nog slimmere methodes, en van rekenmachines. Voor een lijst van Mersenne priemgetallen bekend in september 2008, zie achter in de syllabus.

Van waar deze interesse? Niet om grotere perfecte getallen te maken. Voor Mersenne getallen bestaan er tests die primaliteit onderzoeken. Die tests zijn veel sneller dan voor een willekeurig getal. Zodoende kunnen we grote priemgetallen expliciet construeren.

Ook is er een vermoeden:

(3.6) Vermoeden.? *Er bestaan oneindig veel Mersenne priemgetalen.*

We beginnen steeds beter te begrijpen "waar de Mersenne priemgetallen ongeveer liggen". Als we dat precies zouden kunnen maken, zouden kunnen omsmeden van een heuristische redenering tot een exact bewijs, dan zouden we dit vermoeden misschien kunnen bewijzen. Daarom proberen we met behulp van berekeningen te onderzoeken of onze intuïtie klopt.

(3.7) Binomiaal getallen. We definiëren deze getallen $\binom{n}{i}$ als volgt. Neem een positief geheel getal n.

Voor $i < 0$ en voor $i > n$ schrijven we $\binom{n}{i} = 0$.

Voor $i = 0$ of $i = n$ schrijven $\binom{n}{i} = 1$.

Voor $0 < i < n$ schrijven we $\binom{n}{i}$ voor het aantal mogelijkheden om uit de getallen $\{1, \cdots, n\}$ een deelverzameling van i getallen te kiezen.

Bij voorbeeld: $\binom{n}{1} = n$ en $\binom{n}{n-1} = 1$ (ga na). Bij voorbeeld: $\binom{n}{2} = n{\cdot}(n-1)/2$ voor $n > 1$ (ga na).

Opgave. Bewijs: $\binom{n}{i} = \binom{n}{n-i}$ met behulp van de definitie.

(3.8) Opgave. *Bewijs dat de volgende formule geldt:*

$$\binom{n}{i} \quad = \quad \frac{n!}{(n-i)!\ i!} \quad = \quad \frac{n \times \cdots \times (n-i+1)}{i!}.$$

Hier staat $b!$ (spreek uit: "b faculteit") voor $b! := 1 \times 2 \times \cdots \times b$; we schrijven $1! = 1$ en $0! = 1$.

Opgave. *Bewijs* $\binom{n}{i} = \binom{n}{n-i}$ *met behulp van deze formule.*

(3.9) Opgave. *Bewijs:*

$$\binom{n-1}{i-1} + \binom{n-1}{i} = \binom{n}{i}.$$

Teken de driehoek van Pascal. Deze figuur en het gebruik van binomiaal coëfficiënten was al bekend in de oude Chinese wiskunde (lang vóór Pascal). We zien dat we $\binom{n}{i}$ kunnen bepalen als we $\binom{n-1}{i-1}$ en $\binom{n-1}{i}$ kennen.

Opgave. *Zij p een priemgetal, en $1 < i < p$. Laat zien dat $\binom{p}{i}$ deelbaar is door p.*

(3.10) Opmerking / Opgave. We kunnen zowel (3.7) als (3.8), als (3.9) als definitie van de binomiaal getallen gebruiken (ga na). Uit (3.8) is het helemaal niet duidelijk dat de binomiaal getallen gehele getallen zijn. Maar dat volgt wel uit de andere twee (equivalente) definities.

(3.11) Formule.

$$(X+Y)^n \quad = \quad \sum_{i=0}^{i=n} \binom{n}{i} X^{n-i} Y^i.$$

Opgave. *Bewijs deze formule.* Hier kunnen we definitie (3.7) gebruiken.

Voorbeelden.

$(X+Y)^2 = X^2+2XY+Y^2$, $(X+Y)^3 = X^3+3X^2Y+3XY^2+Y^3$, $(X+Y)^4 = \cdots$ reken uit.

(3.12) Stelling (De kleine stelling van Fermat). *Zij p een priemgetal, en $a \in \mathbb{Z}$. Dan geldt:*

$$a^p \quad \equiv \quad a \pmod{p}.$$

Genoemd "de kleine steling van Fermat" om het verschil aan te duiden met "de laatste stelling van Fermat" (lang een vermoeden, nu bewezen door Andrew Wiles).

De notatie

$$b \quad \equiv \quad c \pmod{n} \qquad \text{betekent:} \qquad b-c \text{ is deelbaar door } n,$$

zie §13.

(3.13) Een bewijs door middel van volledige inductie Veronderstel dat er een bewering $B(j)$ is voor elk positief geheel getal j. we willen al deze bewerkingen bewijzen. Het lijkt alsof we daar oneindig veel tijd voor nodig hebben. In sommige gevallen kan dat korter: een *bewijs met volledige inductie.* Daartoe bewijzen we eerst:
Begin van de inductie. We bewijzen dat $B(1)$ juist is.
vervolgens:
Inductie-stap. Onder aanname dat $m \geq 1$, en onder aanname dat $B(1), B(2), \cdots, B(m)$ allemaal waar zijn bewijzen we dat $B(m+1)$ juist is.
Conclusie. Als de voorgaande stappen met succes voltooid zijn dan volgt $B(i)$ voor elke $i \geq 1$. QED

Een voorbeeld. Bewijs (3.11) met behulp van Definitie (3.9).

(3.14) Bewijs van (3.12). Dit is juist voor $a = 0$.
Als de stelling geldt voor $a > 0$ dan is ook $(-a)^p \equiv (-a) \pmod{p}$ (ga na).
Het is voldoende om de stelling te bewijzen voor een vast gekozen priemgetal p en voor $a \in \mathbb{Z}_{>0}$.

(Begin van de inductie.) *Voor $a = 1$ is de stelling juist.* (Allicht.)
(Inductiestap.) *Als de steling juis is voor $a = j \geq 1$ dan volgt de stelling voor $a = j + 1$.*
Inderdaad, $(j+1)^p$ rekenen we uit met (3.11). we krijgen

$$(j+1)^p = \sum_{i=0}^{i=p} \binom{n}{i} j^{p-i} 1^i = j^p + p \cdot \left(\sum_{i=1}^{i=p-1} \frac{\binom{n}{i}}{p} j^{n-i} 1^i \right) + 1^p.$$

Uit de eigenschappen van de binomiaal coefficiënt $\binom{p}{i}$ en uit de inductie-aanname volgt de conclusie van de inductiestap. QED

(3.15) Bewijs van (3.2). Neem aan dat $q := 2n + 1$ een priemgetal is. Beschouw

$$2 \times (2^n - 1) \times (2^n + 1) = 2^q - 2.$$

uit de kleine stelling van Fermat voor het priemgetal q volgt dat q een deler is van $2^q - 2$. Omdat q priem is en oneven volgt

$$(\text{óf } q \text{ deelt } (2^p - 1)) \qquad (\text{óf } q \text{ deelt } (2^p + 1)).$$

QED

(3.16) Feit*. *Zij $q = 2n + 1$ een oneven priemgetal;*

$$q \equiv 1, 7 \pmod 8 \Longrightarrow q \quad \text{deelt} \quad 2^n - 1;$$

$$q \equiv 3, 5 \pmod 8 \Longrightarrow q \quad \text{deelt} \quad 2^n + 1.$$

In de appendix van deze § geven we een bewijs (waar we niet-elementaire methoden gebruiken).
Was deze regelmaat al opgevallen?
Om dit feit te onthouden: het gedrag is bepaald voor q modulo 8, en:

$$2 \equiv 36 \pmod{17}, \; 2 \equiv 9 \pmod 7$$

en, de kwadraten modulo 3, respectievelijk modulo 5 zijn:

$$\{0, 1\}, \quad \{0, 1, -1\}.$$

(3.17) Gevolg. *Onderstel dat p een oneven priemgetal is met $p \equiv 3 \pmod 8$, zodanig dat $q := 2p + 1$ ook een priemgetal is.*
Als $p \equiv 3 \pmod 4$ dan is q een deler van M_p. Als bovendien $p > 3$ dan is M_p niet een priemgetal.
Inderdaad, want onder deze condities is $q \equiv 1 \pmod 8$ of $q \equiv 7 \pmod 8$; dus is q een deler van M_p. Voor $p > 3$ is bovendien $q < M_p$. QED

Voorbeelden:
M_2 is niet deelbaar door 5;
M_3 is deelbaar door 7, ja allicht, want $M_3 = 7$;

merk op dat $M_5 = 31$ niet deelbaar is door 11
Opgave. Is M_{23} een priemgetal?
Opgave. Vind nog een priemgetal p waarvoor je op deze manier kunt zien dat M_p niet een priemgetal is.
Opgave/Opmerking. Vindt p zodanig dat p priem is, dat $q := 2p+1$ wel priem is, maar zo dat M_p niet priem is.
Opgave. Is 59 een deler van $2^{29}-1$? (Doe een berekening, en/of raadpleeg theorie.)

Appendix*. We schetsen een bewijs van (3.16). Hierbij gebruiken we verwijzingen en methoden die niet elementair zijn.

(3.18) Kwadraatresten. Zij gegeven een priemgetal q en een getal a. We willen graag weten of er een getal b bestaat zodanig dat

$$a \equiv b^2 \pmod q.$$

Als dit zo is dan noemen we a een kwadraatrest modulo q. Voor kleine q kunnen we de kwadraten eenvoudig opschrijven:
voor $q = 3$ zijn $0, 1$ kwadraatresten,
voor $q = 5$ zijn $0, 1, 4$ kwadraatresten,
voor $q = 7$ zijn $0, 1, 4, 2$kwadraatresten, en bv.
voor $q = 17$ zijn $0, 1, 4, 9, 16, 8, 2, 15, 13$ kwadraatresten
(en merk op dat voor $q = 2m+1$ het aantal kwadraatresten gelijk is aan $m+1$).

We willen graag een snel middel hebben om voor een gegeven q (denk aan een groot priemgetal) en een gegeven a te beslissen of a een kwadraatrest modulo q is. De *kwadratische reciprociteitswet* geeft een dergelijk antwoord. We verwijzen naar [78], Hoodstuk 9, of bv. naar [7], Hoofdstuk 11 voor resultaten en bewijzen. Hier is een bijzonder geval wat we nodig hebben:

(3.19) Feit*. *Het getal* 2 *is*
wel een kwadraatrest modulo een priemgetal q
als $q \equiv 1 \pmod 8$ *of als* $q \equiv 7 \pmod 8$,
niet een kwadraatrest modulo een priemgetal q
als $q \equiv 3 \pmod 8$ *of als* $q \equiv 5 \pmod 8$.
We geven niet een bewijs. Zie bij voorbeeld [78], Theorem 9.4.

(3.20) Feit*. *Voor elk priemgetal* q *is de multiplicatieve groep* $(\mathbb{Z}/q)^*$ *cyclisch.*
Zie **??**.
Hiermee bedoelen we het volgende. Kies een priemgetal q. Beschouw de verzameling $\{i \mid 0 < i < q\}$ deze elementen kunnen we vermenigvuldigen "modulo q". We krijgen zo een groep. Voor meer details zie §15. Dat deze groep cyclisch betekent dat er bestaat een r zodanig dat de elementen $\{r, r^2, \cdots, r^i, \cdots, r^{q-2}, r^{q-1}\}$ modulo q precies de verzameling $\{i \mid 0 < i < q\}$ is; bovendien . Zie bv. [7], St. 7.4.1; een getal r met deze eigenschap heet een "*primitieve wortel* modulo q". $r^{q-1} \equiv 1 \pmod q$. **Een voorbeeld.** Neem

$p = 7$ en $r = 5$. Merk op dat de getallen $5, 5^2, 5^3, 5^4, 5^5, 5^6$ in deze volgorde modulo 7 de getallen $5, 4, 6, 2, 3, 1$ zijn.
Opgave. Vind nog een ander getal wat voor $p = 7$ een primitieve wortel is.

Een voorbeeld/Opgave. Neem $q = 17$ en neem $r = 3$. Ga na dat de getallen $r^j \bmod 17$ precies de verzameling $\{i \mid 0 < i < 17\}$ vormen.

(3.21) Een bewijs van (3.16). Neem $q = 2n + 1$ een oneven priemgetal. In (3.12) en (3.15) zagen we dat

$$2^q \equiv 2 \pmod{q};$$

omdat q een oneven priemgetal is volgt uit $q \mid 2^q - 2$ dat q een deler is van $2^{q-1} - 1 = (2^n + 1)(2^n - 1)$. Dus is q een deler van $(2^n + 1)$ óf van $(2^n - 1)$ (en niet van allebei). Het is voldoende om er bewijzen:

$$\exists\, b : \quad 2 \equiv b^2 \pmod{q} \quad \Longleftrightarrow \quad q \mid 2^n - 1.$$

Eerst bewijzen we "($\Rightarrow$)". — Als $2 \equiv b^2 \pmod{q}$ met $b \equiv r^j \pmod{q}$ dan is

$$2^n \equiv r^{2jn} \pmod{q}, \quad 2^n \equiv +1 \pmod{q}.$$

Vervolgens bewijzen we "$\Leftarrow$". — Onderstel $2^n \equiv +1 \pmod{q}$. Schrijf $2 \equiv r^k \pmod{k}$. Als k oneven zou zijn, $k = 2s + 1$ dan zien we $r^{nk} = (r^{2n})^s {\cdot} r^n$, en we concluderen $2^n \equiv -1 \pmod{q}$. Een tegenspraak. Dus voor $k = 2m$, geldt

$$2^n \equiv +1 \pmod{q} \quad \Longrightarrow \quad 2 \equiv (r^m)^2 \pmod{q}.$$

QED (3.16)

Terzijde. We zien dat voor veel priemgetallen het getal $r = 2$ een primitieve wortel is voor het priemgetal p, bij voorbeeld $p = 3, \ = 5, \ = 11, \ = 19$, etc ?.

(3.22) **Vermoeden** (E. Artin). Het getal $r = 2$ is een primitieve wortel voor oneindig veel priemgetallen.
Ze [7], 7.14.3.

4 Meetkundige constructies

We zullen de uitdrukking “constructie” of “meetkundige constructie” gebruiken voor “constructie met passer en lineaal” (en andere constructie methoden, historisch heel interessant, zullen buiten beschouwing blijven). Hieronder verstaan we het volgende.

(4.1) Definitie. We werken in het vlak $\mathbb{R} \times \mathbb{R}$ (bestaande uit alle punten waarvan de coördinaten gelegen zijn in het lichaam $\mathbb{R}$ van de reële getallen). In dat vlak hebben we gegeven twee verschillende punten, bij voorbeeld $(0,0)$ en $(1,0)$. Een **constructie** bestaat uit een eindig aantal stappen en elk van de stappen is een van de volgende, waar we gebruik maken van punten, lijnen en cirkels die al eerder geconstrueerd zijn:

- Met een lineaal trekken we een lijn die gaat door twee punten.
- Voor een gegeven punt M en voor de afstand $r > 0$ tussen twee gegeven verschillende punten tekenen we de cirkel met middelpunt M en straal r.
- Voor twee gegeven, verschillende lijnen die niet evenwijdig lopen bepalen we het snijpunt.
- Voor een gegeven lijn en een gegeven cirkel bepalen we de snijpunten / het raakpunt (die verzameling kan leeg zijn; we werken over $\mathbb{R}$).
- Voor twee gegeven cirkels bepalen we alle snijpunten (die verzameling kan leeg zijn; we werken over $\mathbb{R}$).

We zullen zeggen dat een getal $\alpha \in \mathbb{R}$ construeerbaar is als het optreedt als lengte van een lijnstuk na een eindig aantal stappen.

(4.2) Bewijs dat de volgende constructies mogelijk zijn.
(a) Als we uit de verzameling van reeds geconstrueerde punten een keuze maken van twee punten, dan kunnen we het middelpunt van dat lijnstuk bepalen.
(b) Als we een van de hoeken beschouwen die we krijgen door twee snijdende lijnen te beschouwen (reeds geconstrueerd) dan kunnen we de bissectrice van die hoek construeren.
(c) Als we een lijn en een punt op die lijn (reeds geconstrueerd) beschouwen dan kunnen we de loodlijn in dat punt op die lijn construeren.
(d) Als we een lijn en en punt niet op die lijn (reeds geconstrueerd) beschouwen, dan kunnen de loodlijn vanuit dat punt op die lijn construeren.
(e) Bewijs dat de som van twee construeerbare getallen construeerbaar is.
(f) Bewijs dat het product van twee construeerbare getallen construeerbaar is.
(g) Laat α en $\beta \neq 0$ construeerbare getallen zijn. Laat zien dat α/β construeerbaar is.

(4.3) Definitie. Een veelhoek in het vlak heet regelmatig als alle zijden onderling gelijke lengte hebben, en alle hoeken onderling gelijke grootte hebben.

(4.4) Stel reeds geconstrueerd een cirkel. Bewijs dat de volgende constructies mogelijk zijn.
(a) Een regelmatige 3-hoek ingeschreven in die cirkel.
(b) Voor elke $i \in \mathbb{Z}_{>1}$ een regelmatige n-hoek met $n = 2^i$ ingeschreven in die cirkel.
(c) Voor elke $j \in \mathbb{Z}_{>0}$ een regelmatige m-hoek met $m = 2^i \times 3$ ingeschreven in die cirkel.
(d) **Opmerking.** We zullen zien dat een regelmatige 5-hoek geconstrueerd kan worden. Dus ook een regelmatige k-hoek met $k = 2^i \times 5$.

Dit waren de constructie reeds bekend vanuit de klassieke Griekse wiskunde. Daar werden ook de volgende vragen gesteld:

(4.5) Vragen.

- **Verdubbeling van de kubus.** Gegeven een eenheids-lengte 1. Kunnen we een getal $\alpha \in \mathbb{R}_{>0}$ construeren zodanig dat een kubus waar van de ribben lengte α hebben als inhoud 2 heeft? M.a.w. is $\sqrt[3]{2}$ constreerbaar?

- **Kwadratuur van de cirkel.** Gegeven een cirkel met straal van lengte 1. Kunnen we een vierkant maken waarvan het oppervlak gelijk is aan dat van de cirkel? M.a.w. is $\sqrt{\pi}$ constreerbaar?

- **Trisectie van elke hoek.** Kunnen we een hoek van 20^o construeren? Kunnen we een willekeurige hoek in 3 gelijke delen verdelen?

- **Constructie van regelmatige veelhoeken.** Voor welke getallen $n > 2$ kunnen we een regelmatige n-hoek construeren?
  Ga na. Dit is equivalent met: voor welke waarde van m kunnen we de hoek $360/m^0$ construeren ?

(4.6) Antwoorden. Deze vragen zijn tenslotte allemaal beantwoord.

- **Verdubbeling vande kubus.** Het getal $\sqrt[3]{2}$ is niet constreerbaar. (Ik hoop in de behandeling van § 7 en van § 15 daar iets over de zeggen.

- **Kwadratuur van de cirkel.** Johann Heinrich Lambert bewees in 1761 dat π niet een rationaal getal is. Maar dat is niet voldoende om te beslissen over de kwadratuur van de cirkel. In 1882 bewees Carl Louis Ferdinand von Lindemann dat π een transcendent getal is. Dit wil zeggen dat π niet nulpunt is van een polynoom. Gevolg: de kwadratuur van de cirkel is niet mogelijk.

- **Trisectie van elke hoek.** Een hoek van 20^o kunnen we niet met passer en lineaal construeren? We kunnen niet elke hoek met passer en lineaal in drie gelijke delen verdelen. Ik kom daar nog op terug.

- **Constructie van regelmatige veelhoeken.** De onderstaand stelling van Gauss vertaalt dit probleem in een (lastig) open probleem over het al of niet priem zijn van Fermat getallen.

(4.7) Stelling (Gauss, 29-III-1777, 1801). *Zij $n \in \mathbb{Z}_{\geq 3}$. Een regelmatige n-hoek is te construeren met passer en lineaal dan en slechts dan als er bestaan $i \geq 0$, $s \geq 0$ en Fermat priemgetallen $p_1 < p_2 < \cdots < p_s$ met $n = 2^i \times p_1 \times \cdots \times p_s$.*

Inderdaad, op 18-jarige leeftijd zag Gauss dat een regelmatige 17-hoek te construeren is (op een ochtend, nog in bed). Later in zijn *Disquisitiones Arithmeticae*, gepubliceerd in 1801, annonceert hij bovenstaande stelling.

Heeft Gauss inderdaad deze stelling volledig bewezen? Een interessante historische vraag. Zie David L. Clements – *An historical contradiction*, Missouri Journal of Mathematical Sciences Articles, **8**, 1996,
zie http://www.math-cs.cmsu.edu/ mjms/1996-2p.html
het is een verwijzing in
http://en.wikipedia.org/wiki/Constructible_polygon
Zie ook http://www.jstor.org/view/00029890/di991533/99p22436/0

Nog interessanter vind ik de volgende vraag. Gauss ziet als 18-jarige waarschijnlijk een belangrijk hulpmiddel, 30 jaar later ontwikkeld door Galois, en nu bekend als "Galoistheorie" (bij voorbeeld een van de belangrijkste hulpmiddelen bij het bewijs van FLT, maar ook van ongelooflijk nut in andere beschouwingen). Ik denk dat Gauss volledig in staat was die theorie te ontwikkelen. Maar Gauss laat het bij een bijzonder geval (Galois theorie toegepast op een uitbreiding $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$), zonder de algemenere aspecten na te gaan. Ik denk dat Gauss hier typisch een "probleem-oplosser" is, en niet een wiskundige is die onmiddelijk de algemenere theorie achter het voorbeeld bestudeerd. Het zou mooi en interessant zijn om dit aspect in zijn algemeenheid historisch verder te onderzoeken.

Ook hier zien we dat een stelling twee schijnbaar verschillende zaken in de wiskunde met elkaar in verband worden gebracht. Hier de construeerbaarheid van een regelmatige p-hoek, en de vraag of p een Fermat priemgetal is.

Het probleem van verdubbeling vande kubus, trisectie van een hoek, en constructie van regelmatige veelhoeken werd in 1837 volledig opgelost door Wantzel, zie [96].

5 Fermat priemgetallen

In deze paragraaf maken we een curieuze overstap: van "meetkundige constructies" naar "bepaalde priemgetallen". We hebben gezien dat priemgetallen van de vorm 2^j+1 interessant zijn. Eerst een eenvoudig resultaat:

(5.1) Lemma. *Als $j = r{\cdot}t$ met $r \in \mathbb{Z}_{\geq 3}$, $t \in \mathbb{Z}_{\geq 1}$ en r is oneven, dan is $2^j + 1$ niet een priemgetal.*
Anders gezegd: als $2^s + 1 = p$ een priemgetal is, dan is p van de vorm:

$$p = 2^{2^i} + 1.$$

Bewijs. Merk op: voor

$$2^j+1 = 2^{r\cdot t}+1 \quad = \quad \left(2^{(r-1)t} - 2^{(r-2)t} + \ldots + (-1)^{k-1}2^{(r-k)t} + \cdots + 2^t - 1\right)\cdots(2^t+1);$$

dit mogelijk omdat $r > 1$ en r is oneven. We zien dat $1 < 2^t + 1 < 2^{r\cdot t} + 1$. We concluderen dat dit een factorizatie van $2^j + 1$ geeft. QED

(5.2) Notatie/Definitie. We schrijven

$$F_i := 2^{2^i}, \quad i \in \mathbb{Z}_{\geq 0}; \quad F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537, \cdots \quad .$$

Dit heten de Fermat getallen. Als F_i een priemgetal is, dan heet dit een Fermat priemgetal.

Merk op dat de Fermat getallen met groeiende i al snel heel groot worden. We zien dat F_8 al een getal is van 78 cijfers.

Hoe kunnen we eenvoudig schatten hoeveel het aantal cijfers van een Fermat getal ongeveer is? We kunnen gebruiken dat $2^{10} = 1024$. Daaruit zien we dat

$$2^{60} > 1000^6 = 10^{18}; \quad \text{inderdaad} \quad 10^{18} < 2^{60} < 2^{19}.$$

We gebruiken dit en we zien dat

$$F_8 = 2^{256} + 1 > (2^{60})^4 \times 2^{16} > 10^{72} \times 65536 > 10^{76}.$$

We kunnen ook gebruiken:

$$^{10}\log(2) \approx 0.301029996.$$

Dus

$$^{10}\log(2^{256}) \approx 256 \ \times \ 0.301029996 \approx 77.06367889.$$

(5.3) Opgave. Gebruik $^{10}\log(3) \approx 0.477121255$ om een afschatting te geven van 3^{1600}.

(5.4) De stelling van Gauss over de constreerbaarheid van regelmatige n-hoeken kunnen we nu formuleren als:

een regelmatige n-hoek is contrueerbaar met passen lineaal dan en slechts dan als $n \geq 3$ en

$$n = 2^a \cdot F_{b_1} \times \cdots \times F_{b_k}, \quad a, k \in \mathbb{Z}_{\geq 0},$$

,

met $F_{b_1} < \cdots < F_{b_k}$ onderling verschilende priemgetallen.

Om het meetkundige probleem op te lossen is het dus voldoende om van de Fermat getallen te beslissen welke priem zijn. Fermat hoopte zo een formule te vinden voor oneindig veel priemgetallen. Echter Euler bewees:

(5.5) Euler, 1732: $F_5 = 4294967297$ is niet een priemgetal.
Bewijs. Dit volgt uit de identiteit:

$$F_5 = 4294967297 = 641 \times 6,700,417.$$

Maar we geven liever een verklaring waarom die factor 641 inderdaad een deler is van F_5 (hierin volgen we Euler). Merk op:

$$641 = 5 \cdot 2^7 + 1 = 625 + 16 = 5^4 + 2^4.$$

We zien

$$5^4 \cdot 2^7 \equiv -1 \pmod{641}; \quad \left(5^4 \cdot 2^7\right)^4 \equiv +1 \pmod{641}; \quad 5^4 \equiv -2^4 \pmod{641}.$$

Dus, voor $F_5 = 2^{32} + 1$ geldt:

$$-2^4 \cdot 2^{28} \equiv +1 \pmod{641}; \quad \text{dus} \quad F_5 \equiv 0 \pmod{641}.$$

QED

Waarom geven we deze laatste berekening? Omdat dit een weg opent om onhandelbare grote getallen zoals F_i aan te pakken:

(5.6) Stelling. *Elk priemgetal p dat F_i deelt, met $i \geq$ is van de vorm:*

$$p \equiv 1 \pmod{2^{i+1}}.$$

Bewijs*. (Hier gebruiken we een iets geavanceerde theorie.) Om dat p een deler is van F_i volgt

$$(2 \pmod{p})^{2^i} = -1 \quad \text{in} \quad \mathbb{F}_p^*.$$

hier uit volgt dat de orde van $2 \pmod{p} \in \mathbb{F}_p^*$ gelijk is aan 2^{i+1}. Dus 2^{i+1} deelt $p - 1$. QED

(5.7) **Euler.** Dit kunnen we verscherpen:

$$i > 1, \quad p|F_i \quad \Longrightarrow \quad p \equiv 1 \pmod{2^{i+2}}.$$

Nu we dit weten kunnen we naar delers gaan kijken, en het vereenvoudigt het zoeken naar delers van Fermat getallen. Bij voorbeeld van F_5: we testen $p \stackrel{?}{=} 1+k.2^7$, $2^7 = 128$:

$k = 1$, 3 deelt $1 + 128$;
$k = 2$, $1 + 2{\cdot}128 = F_3$, en dit getal is priem met F_5;
$k = 3$, 5 deelt $1 + 3{\cdot}128$;
$k = 4$, 3 deelt $1 + 4{\cdot}128$;
$k = 5$, $p = 1 + 5{\cdot}128$, AHA.

Zo is het opsporen van delers van F_i gemakkelijker geworden.

(5.8) Status:

er is geen Fermat priemgetal bekend met $i > 4$;
we weten niet of er oneindig veel i zijn zo dat F_i niet priem is,
we weten niet of er oneindig veel i zijn zo dat F_i wel priem is.
Van een aantal Fermat getallen is de volledige factorizatie bekend.
Van soms hele grote Fermat getallen is bekend dat ze niet priem zijn.

Van F_{33} is nu niet bekend of dit een priemgetal is. (Hoeveel cijfers heeft dit getal ?)
Zie verder (9.7).

Een voorbeeld: $F_{2478782}$ is niet een priemgetal. (Dit is een onvoorstelbaar groot getal. Kunt u een schatting van het aantal cijfers geven?)
Een voorbeeld: News Flash! On January 10, 2009 Takahiro Nohara discovered another new factor of a Fermat number: $77795{\cdot}2^{38969} + 1$divides F_{38967}. Zie

http://www.prothsearch.net/fermat.html

Zie verder (9.7). Zie ook:

http://en.wikipedia.org/wiki/Fermat_number
http://mathworld.wolfram.com/FermatPrime.html

(5.9) Een oplossing van (5.3). ${}^{10}\log(3^{1600}) \approx 1600 \times 0.477121255 \approx 763.394007551$.
We zien dat 3^{1600} een getal is van minstens 764 cijfers.

Het aantal cijfers van F_{33}, bereken: $2^{33} \times {}^{10}\log(2) \approx 8589934592 \times 0.301029996 \approx 258582797$

6 De priemgetalstelling

We hebben gezien dat er oneindig veel priemgetallen bestaan (zoals Euclides al lang geleden bewees). In deze paragraaf laten we zien hoe de priemgetallen verdeeld liggen. Elke keer als ik dit weer zie, ben ik verbaasd dat je zinnige dingen kunt zeggen over een oneindige verzameling, waar we van bijna alle elementen ervan niet weten hoe ze er uit zien. Van slechts eindig veel priemgetallen kennen we de precieze vorm. Maar waar ze "ongeveer" liggen weten we vrij precies. Dat gaan we laten zien.

(6.1) We proberen de som van de reeks

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p} + \cdots$$

uit te rekenen. Stel eens dat we het werk van Euler niet kennen, dat we graag op een grote computer rekenen, en dat we aan de slag gaan. Na een tijdje rekenen blijkt de som van eindig veel termen steeds langzamer te groeien. Nadat die snelle computer jaren lang staat te rekenen komen zien we de som nog nauwelijks groeien. Als we $1/p$ opgeteld hebben voor alle $p < 10^9$ dan zien we er minder dan 3.3 als som uit komen. Stel dat we nog voldoende geduld en rekencapaciteit hebben, dan zien we dat die som minder is dan 4 voor alle $p < 10^{18}$.

Zouden we zo'n berekening ooit willen doen?
Het aantal priemgetallen met $p < 10^{18}$ is ongeveeer 24×10^{15}.

(Om precies te zijn: 24,739,954,287,740,860.)

Als we vertrouwen zouden hebben in de heuristiek van zulke berekeningen dan zouden we al gauw concluderen dat de som begrensd is als we over alle priemgetallen zouden sommeren. Veel rekenwerk, geen denkwerk.... we zullen zien dat een eenvoudig bewijs heel iets anders laat zien.

(6.2) **Stelling.** **(a)** (De harmonische reeks.) *De reeks*

$$\sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$$

is divergent.
(b) (Euler, 1737). *De reeks*

$$\sum_{p \text{ is priem}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \cdots$$

is divergent.
(c) (Brun) We schrijven $\mathcal{T}$ voor de verzameling van priemgetallen p zodanig dat $q = p+2$ ook een priemgetal is; m.a.w. (p, q) is een priemtweeling. *De reeks*

$$\sum_{p \in \mathcal{T}} (\frac{1}{p} + \frac{1}{p+2}) = (\frac{1}{3} + \frac{1}{5)} + (\frac{1}{5} + \frac{1}{7}) + (\frac{1}{11} + \frac{1}{13}) \cdots$$

is convergent.
(d) *De reeks*

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots$$

is convergent.

Feit:

$$\text{Euler bewees in 1735/1736:} \quad \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Toelichting. Het sommatieteken $\sum$ wordt als volgt gebruikt: eronder en soms ook erboven staat welke index loopt, en wat de grenzen daarvoor zijn; achter het somteken staat wat er gesommeerd wordt.
Convergeert. We zeggen dat $\sum_i a_i$ *convergeert* als er een (eindig) getal σ bestaat, zodat deelsommen daar willekeurig dichtbij komen. In technische termen: voor elke $\varepsilon \in \mathbb{R}_{>0}$ is er een N zodanig dat

$$\mid \sigma - \sum_{i=1}^{i=N} a_i \mid < \varepsilon; \quad \text{we schrijven:} \quad \sum_{i=1}^{\infty} a_i \quad = \quad \sigma.$$

Divergeert. We zeggen dat $\sum_i a_i$ *divergeert* als er voor elke $S \in \mathbb{R}$ een N betaat zodanig dat

$$\sum_{i=1}^{i=N} a_i \quad > \quad S; \quad \text{we schrijven:} \quad \sum_{i=1}^{\infty} a_i \quad = \quad \infty.$$

Het kan voorkomen dat een reeks niet convergeert en niet divergeert.

Waarom deze stelling? We willen (nogmaals) onderzoeken of er eindig of oneindig veel priemgetallen bestaan. De som in (b) is dezelfde als in (a), maar veel termen weggelaten; nog steeds divergent? Hoe bewijs je zoiets, zonder alle priemgetallen te kennen? Uit (b) volgt inderdaad dat er oneindig veel priemgetallen bestaan.

We zouden kunnen proberen om zo te beslissen of er ook oneindig veel priemtweelingen bestaan. Maar de som in (c) convergeert, en we krijgen zo geen uitsluitsel

In (d) dunnen we reeks nog verder uit; we zien in dat geval dat convergentie eenvoudig te bewijzen is.

(6.3) Bewijs van (6.2).a. Merk op:

$$\frac{1}{3} + \frac{1}{4} > \frac{1}{2}, \quad \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} > \frac{1}{2}, \quad \cdots \quad , \frac{1}{2^j + 1} + \cdots + \frac{1}{2^{j+1}} > \frac{1}{2}, \quad \cdots .$$

We zien dat voor $i \geq 2^j$ geldt:

$$\sum_{n=1}^{n=i} \frac{1}{n} \quad > \quad (j+1) \cdot \frac{1}{2}.$$

Dit bewijst (a).

(6.4) Opmerking. Bewezen kan worden:

$$\log(N) < 1 + \frac{1}{2} + \cdots + \frac{1}{N} = \sum_{n=1}^{n=N} \frac{1}{n} < 1 + \log(N), \quad \forall\, N \in \mathbb{Z}_{>1}.$$

Zie [7], St. 21.2.1. We zien "hoe snel" $\sum_{n \leq N} (1/n) \to \infty$ voor $N \to \infty$.

(6.5) Bewijs van (6.2).b. (Nogmaals: hoe kunnen iets zeggen over $\sum_p 1/p$ zonder alle p te kennen ... ?)
Neem aan dat de som in (b) convergeert. In dat geval bestaat er voor $\varepsilon = 1/2$ een getal N zodanig dat

$$\sum_{p \text{ is priem},\ p>N} \frac{1}{p} < \frac{1}{2}.$$

Definieer het getal

$$Q := \prod_{p \text{ is priem},\ p \leq N} p.$$

Merk op dat voor elke $n \in \mathbb{Z}_{\geq 1}$ het getal $1 + nQ$ alleen maar factoren groter dan N bezit. Hieruit volgt dat voor elke $M \in \mathbb{Z}_{\geq 1}$ we de volgende ongelijkheid hebben:

$$\sum_{n=1}^{n=M} \frac{1}{1+nQ} \leq \sum_{t=1}^{\infty} \left(\sum_{p>N} \frac{1}{p} \right)^t ;$$

dit volgt want elke term links komt links maar één keer voor, en komt rechts ook voor (hier gebruiken we de eenduidigheid van factorontbinding). Uit

$$\sum_{t=1}^{\infty} \left(\sum_{p>N} \frac{1}{p} \right)^t \leq \sum_{t=1}^{\infty} \left(\frac{1}{2} \right)^t = 1$$

concluderen we dat

$$\sum_{n=1}^{\infty} \frac{1}{1+nQ}$$

convergent zou zijn. Echter

$$\frac{1}{1+nQ} \geq \frac{1}{n+nQ} = \frac{1}{1+Q} \cdot \frac{1}{n}; \quad \text{dus} \quad \sum_{n=1}^{n=T} \frac{1}{1+nQ} \geq \frac{1}{1+Q} \cdot \sum_{n=1}^{n=T} \frac{1}{n}.$$

Uit (a) volgt dat $\sum_n 1/(1+nQ)$ divergeert; dit is in tegenspraak met de eerdere conclusie. Dit bewijst dat de aanname foutief was; dit bewijst (b).

Opmerking. Het resultaat (b) werd bewezen door Euler. Maar wat is nu de verklaring dat die som zo langzaam groeit, zoals we bij een lange computerberekening geconstateerd zouden hebben? Gauss vermoedde het volgende asymptotische gedrag in 1796 en Mertens bewees dit vermoeden in 1874:

$$\sum_{p \text{ is priem},\ p<x} \frac{1}{p} = \log\log x + C + \varepsilon(x),$$

met $\varepsilon(x) \to 0$ voor $x \to \infty$; hier is log de logaritme met grondtal e en de constante C is ongeveer 0.261497 . Bij voorbeeld: $\log(10^{18}) \approx 41.45$ en $\log(\log(10^{18})) \approx 3.72$. Vandaar dat $\sum_{p<N}$ zo langzaam groeit voor $N \to \infty$.

(6.6) **Over** (6.2).c. Dit is een mooi resultaat van V. Brun, zie [9]: er is een constante B zodanig dat

$$\sum_p \frac{1}{p} \quad = \quad B; \quad \text{men verwacht:} \quad B \approx 1.902160583 \quad .$$

We zullen dit resultaat niet bewijzen. Zie:
http://numbers.computation.free.fr/Constants/Primes/twin.html

(6.7) **Bewijs van** (6.2).d. Merk op:

$$(1/4) + (1/9) < 1/2, \quad \text{en} \quad (1/16) + \cdots + (1/49) < 4{\cdot}(1/16), \quad \cdots .$$

Algemeen:

$$(\frac{1}{2^i})^2 = \frac{1}{2^{2i}}, \quad \text{en} \quad \frac{1}{2^{2i}} + \cdots + (\frac{1}{2^{i+1}-1})^2 \quad < \quad 2^i{\cdot}\frac{1}{2^{2i}} \quad = \quad \frac{1}{2^i}.$$

Conclusie:

$$\sum_{n=1}^{\infty} \frac{1}{n} \quad < \quad 1 + \sum_{i=1}^{\infty} \left(\frac{1}{2}\right)^i = 2.$$

Dit bewijs convergentie van $\sum_n (1/n)$.

De precieze waarde van deze som werd reeds door Euler bewezen. Een bewijs en verwijzingen vinden we in:
http://mathworld.wolfram.com/RiemannZetaFunctionZeta2.html
Dit is het einde van het bewijs van (6.2).

(6.8) **Notatie.** We schrijven $\pi(-)$ voor de reële functie gedefinieerd door:

$$\pi(x) \quad = \quad \#\left(\{p \mid p \quad \text{is priem}, \quad p \leq x\}\right), \quad \forall x \in \mathbb{R}.$$

De notatie $\#(V)$ wordt gebruikt voor het aantal elementen van de verzameling V. Dat lijkt niet een erg mooie functie, het is een "trapfunctie". Voor $x < 2$ is $\pi(x) = 0$, voor $2 \leq x < 3$ is $\pi(x) = 1$, en zo voort: bij elk priemgetal springt de functiewaarde met 1 omhoog.

Veel wiskundigen zijn gefascineerd door deze functie. Als je deze functie uitzet op een grote schaal, zodat je de discontinuïteiten niet meer ziet, dan komt er een mooi gladde functie uit, zie [100], pp. 6 en 7. Kunnen we die functie (ongeveer) beschrijven?

Op grond van de eerste berekeningen, en met behulp van een logaritme tabel die hij gekregen had vermoedde de 15-jarige Gauss het asymptotisch gedrag van $\pi(-)$. Gauss besteedde vaak elk "vrij kwartier" aan het uitrekenen van steeds meer priemgetallen.

In zijn leven bepaalde hij alle priemgetallen onder $3,000,000$. Natuurlijk wist hij ok wel dat een dergelijk asymptotisch gedrag niet door een eindige berekening zou kunnen aantonen. Maar hij wilde graag dat het experiment zijn vermoeden zou ondersteunen; steeds vergeleek hij de uitkomst van zijn berekeningen (het aantal priemgetallen onder een gegeven grens) met zijn vermoeden.

(6.9) De priemgetalstelling*.

$$\boxed{\pi(x) \quad \sim \quad \tfrac{x}{\log(x)}.}$$

Uitleg. Hiermee bedoelen we:

$$\lim_{x\to\infty} \quad \frac{\pi(x)}{x/\log(x)} \quad = \quad 1.$$

Pas op. De notatie zegt niet dat het verschil $|\ \pi(x) - x/\log(x)\ |$ naar nul gaat.
We zullen geen bewijs hiervan geven, dat ligt ver buiten de mogelijkheden van dit college.

Dit resultaat werd door Legendre vermoed in zijn "Essai sur le théorie des nombres in 1798. Stelling (6.9) werd vermoed door Gauss waarschijnlijk rond 1791 (of 1793?); Gauss beschrijft dit in een brief aan Enke, 1849 en Gauss publiceert dit in 1863. De formules die Gauss en Legendre gebruikten zijn in een iets andere vorm dan hierboven vermeld, maar ze geven hetzelfde asymptotische resultaat.

In 1848 en 1850 bewees Chebyshev een zwakke vorm van deze stelling, zie (6.13).
Riemann schreef in 1859 een artikel over dit onderwerp, [76]. Dat artikel is van een enorme invloed op de ontwikkeling van de wiskunde. Het bevat een vermoeden, nu genoemd "de Riemann Hypothese", nog steeds onbewezen, een van de belangrijkste vermoedens in de wiskunde. Een artikel van 9 bladzijden, en nog zijn we aan het denken en werken aan wat daarin aan de orde wordt gesteld.
Hadamard en De la Vallée Poussin werkten verder aan dit onderwerp, zoals gesuggereerd door Riemann, de analytische benadering van de verdeling van priemgetallen, en zij bewezen deze stelling, onafhankelijk van elkaar, in 1896. Pas in de 20-ste eeuw werd deze stelling PNT genoemd, de "Prime Number Theorem".
Daarna werden nog vele bewijzen gevonden. Daaronder in 1949 "elementaire bewijzen" door Selberg en door Erdös (elementair slaat erop dat er geen diepe methoden van de analytische getaltheorie bij het bewijs gebruikt worden, maar deze bewijzen zijn niet "eenvoudig").
Zie:

http://en.wikipedia.org/wiki/Prime_number_theorem
http://primes.utm.edu/howmany.shtml
http://oregonstate.edu/ peterseb/misc/docs/pnt.pdf

Op de volgende site kunt U het artikel van Riemann het manuscript, de gedrukte versie, en een vertaling ervan vinden:

http://www.claymath.org/millennium/Riemann_Hypothesis/1859_manuscript/

(6.10) De versies van Legendre en van Gauss zijn iets verschillend.
Legendre:

$$\pi(x) \sim x/(\log(x) - 1.08366).$$

Dit is equivalent met de PNT. De constante 1.08366 baseerde Legendre op een beperkte lijst van waarden van π die hem toch beschikking stonden: $x < 400,000$. Voor grote waarden van x is $x/\log(x)$ een betere benadering.

Gauss gebruikte de functie $Li(x)$ (de hoofdwaarde van de integraal van $1/\log(u)$ van $u = 0$ tot $u = x$), en zijn vermoeden was dat $\pi(x) \sim Li(x)$. Dit vermoeden is ook equivalent met (6.9). De benadering van Gauss is iets beter dan die van Legendre.

(6.11) **Amusant detail.** Uit tabellen lijkt het alsof $Li(x) > \pi(x)$ zou gelden voor alle waarden van x. Echter, Littelwood bewees in 1914 dat $Li(x) - \pi(x)$ oneindig vaak van teken wisselt voor groeiende x. Waarom zagen we dat niet in tabellen? Skewes bewees dat er een x bestaat met met

$$x < \text{ tweede getal van Skewes} := 10^{10^{10^{963}}}$$

waarvoor $Li(x) < \pi(x)$. Later werd deze grens verscherpt; bij voorbeeld Te Riele bewees in 1987 dat het teken wisselt voor een $x < 7 \times 10^{370}$. Maar Kotnik bewees in 2008 dat

$$(x < 10^{14}) \quad \Longrightarrow \quad (Li(x) > \pi(x)),$$

vandaar.

(6.12) De PNT (priemgetal stelling) is een diepe stelling, een triomf van een suggestie van Riemann, en diepe analytische getaltheorie uit de 19-de eeuw. Er is een versie die heel goed bruikbaar is, weliswaar zwakker, en waarvan bovendien een elementair bewijs gegeven kan worden:

(6.13) **Stelling.** *Er is een geheel getal $N \in \mathbb{Z}_{>0}$ en er zijn $A, B \in \mathbb{R}$ met $0 < A < 1 < B$ zodanig dat:*

$$A \cdot \frac{x}{\log(x)} < \pi(x) < B \cdot \frac{x}{\log(x)}, \quad \forall \;\; x \geq N.$$

Voor het eerst bewezen door Tschebyscheff in 1849 met $A = 89/100$ en $B = 111/100$.

Rosser (1941), zie [79] :

$$\frac{x}{\log x + 2} < \pi(x) < \frac{x}{\log x - 4} \qquad x \geq 55.$$

In [100] vinden we:

$$\frac{2}{3} \cdot \frac{x}{\log(x)} < \pi(n), \quad \forall \;\; n > 200$$

$$\pi(n) < \frac{17}{10}\cdot\frac{x}{\log(x)}, \quad \forall \; n \in \mathbb{Z}.$$

Eenvoudig te bewijzen, zie [3], Th. 4.6:

$$\frac{1}{6}\cdot\frac{x}{\log(x)} < \pi(n) < 6\cdot\frac{x}{\log(x)}, \quad \forall \; n > 2.$$

(6.14) Met behulp van methoden zoals vermeld in (6.13) kunnen we *schattingen* geven van het aantal priemgetallen op een gegeven interval: voor een interval ter lengte D van gehele getallen geldt:

$$\pi(n + (D/2)) - \pi(n - (D/2)) \quad \approx \quad \frac{D}{\log(n)}.$$

Deze schattingen zijn uitermate precies, zie bv [65] en verwijzingen daar, of zie (6.20).

We kunnen ook preciese aantallen geven. Voor reële getallen $x < y$ schrijf

$$\pi(x, y) = \#\left(\{p \mid \; p \text{ is priem}, \quad x < p \leq y\}\right).$$

Gebruikmakend van (6.13) zien we:

$$A\cdot\frac{y}{\log(y))} - B\cdot\frac{x}{\log(x))} < \pi(x, y) < B\cdot\frac{y}{\log(y))} - A\cdot\frac{x}{\log(x))}.$$

Als we grote getallen beschouwen, dan kunnen we A en B dicht bij 1 kiezen. Als we dan x veel kleiner kiezen dan y (een groot interval), dan komen er goede afschattingen.

(6.15) We nummeren alle priemgetallen:

$$p_1 = 2 < p_2 = 3 < p_3 = 5 < \cdots < p_i < p_{i+1} < \cdots \; .$$

(6.16) Stelling.*

$$\boxed{p_n \quad \sim \quad n \log(n)}$$

(6.17) Stelling (6.9) en Stelling (6.16) zijn logisch equivalent: de ene impliceert de ander, en omgekeerd; zie bv. [3], Th. 4.5

(6.18) Stelling. *Er is een geheel getal $M \in \mathbb{Z}_{>0}$ en er zijn $C, D \in \mathbb{R}$ met $0 < C < 1 < D$ zodanig dat:*

$$C\cdot n \log(n) < p_n < D\cdot n \log(n), \quad \forall \; n \geq M.$$

(6.19) Stelling (6.13) en Stelling (6.18) zijn logisch equivalent: de ene impliceert de ander, en omgekeerd. Dit is gemakkelijk in te zien:

Ga uit van $\pi(x) < B\cdot x/\log(x)$ en concludeer $(1/B)\cdot n \log(n) < p_n$ (voor $x, n > \cdots$).
Ga uit van $A\cdot x/\log(x) < \pi(x)$ en concludeer $p_n < (1/A)\cdot n \log(n)$ (voor $x, n > \cdots$).

(6.20) De "kans" dat een getal n priem is is ongeveeer $1/\log(n)$. Deze uitspraak is niet erg zinvol. We bedoelen ermee: geef een "groot" interval rond n, tel het aantal priemgetallen in dat interval, en deel door de lengte van het interval; het resulterende getal ligt dicht bij $1/\log(n)$.
Voorbeeld. Neem als interval $[10^8, 10^8 + 150000]$. Dan geldt

$$\#\left(p \mid 10^8 < p < 10^8 + 150000\{\}\right) \quad = \quad 8154$$

(een gigantische rekenpartij). Een schatting levert:

$$\frac{150000}{\log 10^8} \approx 8143.$$

Dat is er niet ver naast. Pas op, dit is een *schatting en geen bewijs* dat er ten minste een priemgetal op dit interval ligt.

(6.21) *We laten zien:* $p_n < 10^n, \ \forall n.$
We schetsen het bewijs. Gebruik (6.13). Uit $A[\cdot]x/\log(x) < \pi(x$ volgt door substitutie $x = p_n$ dat

$$p + n < \frac{1}{A} \cdot n \cdot \log(p_n).$$

We nemen $A = 2/3$. Omdat $\log(y) < (2/3)\sqrt{y}$ komt er

$$p_n < \frac{2}{3} n \frac{3}{2} \sqrt{p_n}.$$

Dus

$$p_n < n^2 < 10^n.$$

We kunen beginnen met de eerste vergelijking met $n > 200$. De andere ongelijkheden gelden dan onder die voorwaarde. Voor $2 \leq n \leq 200$ zien we dat $p_n < 3n\log(n)$ en $p_n < n^2$ uit tabellen. QED

(6.22) **Opgave.** Bewijs dat er een priemgetal bestaat met 19 cijfers.

(6.23) **Opgave.** Bewijs dat er een priemgetal ligt tussen 10^8 en 3×10^8.

(6.24) **Opgave** (H. W. Lenstra). Bewijs dat er oneindig veel waarden van n zijn zodanig dat $\pi(n)$ een deler is van n. (Dit lijkt toch fantastisch, zo iets bewijzen zonder alle waarden van $\pi(-)$ te kennen ?)

(6.25) **Een oplossing van** opgave (6.22). We kunnen in de tabel van Mersenne priemgetallen kijken, en we zien dat $M_{61} = 2^{61} - 1$ een priemgetal is, en 19 cijfers heeft.

We kunnen ook een heel ander bewijs geven. Laten we gebruiken dat

$$(2/3) \cdot x\log(x) < \pi(x) < (17/10) \cdot x\log(x).$$

Dan zien we:

$$\pi(10^{20}) > \frac{2}{3} \cdot 10^{20} \log(10^{20}) = \left(\frac{2}{3} \times 10 \times 20\right) \times \left(10^{19} \times \log(10)\right)$$

en

$$\pi(10^{19}) < \frac{17}{10} \cdot 10^{19} \log(10^{19}) = \left(\frac{17}{10} \times 19\right) \times \left(10^{19} \times \log(10)\right)$$

Omdat

$$\frac{2}{3} \times 10 \times 20 = \frac{400}{3} > \frac{323}{10} = \frac{17}{10} \times 19 \quad \text{volgt} \quad \pi(10^{20}) > \pi(10^{19}).$$

QED

Dit is toch overtuigend. Met practisch geen rekenwerk laten we zien dat er een dergelijk priemgetal bestaat.

(6.26) Een beter voorbeeld: een oplossing van Opgave (6.23).

$$\pi(3 \times 10^8) > \frac{2}{3}(3 \times 10^8) \log(3 \times 10^8) > 2 \times 10^8 \times \log(10^8) > \frac{17}{10} 10^8 \times \log(10^8) > \pi(10^8).$$

(6.27) Een hint voor Opgave (6.24). Gebruik dat $\lim_{n \to \infty} \pi(n)/n = 0$.

7 Iets over het bewijs: construeerbaarheid van regelmatige veelhoeken*

In deze paragraaf zal ik op het colege iets zeggen over de trisectei van de hoek, en de constructie van regelmatige veelhoeken. De constructie van een regelmatige 5-hoek is klassie, en eenvoudigte geven. Het bewijs dat trisectie in het algemeen niet mogeijk is, en een bewijs van Stelling (4.7) is niet elementair. Ik zal proberen er iets over te zeggen.

8 Sophie Germain

Op het college zal ik iets vertellen over de wiskundige Sophie Germain. Enkele verwijzingen:

[63] Een prachtiug boek van Dora Musielak over haar met een fictieve beschrijving van haar dagboek van haar 13-de tot haar 17-de jaar ("historische fictie").

Een stuk van Mary W. Gray, zie [40], met een korte levensbeschrijving.

[10] Een fascinerende berschrijving van haar leven, en de weg die leidde tot het verkrijgen van een prestigieuze prijs.
Zie ook:
http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Germain.html
http://www.agnesscott.edu/Lriddle/WOMEN/germain.htm
http://en.wikipedia.org/wiki/Sophie_Germain

Hier is een steling bewezen door haar.

(8.1) Stelling (Sophie Germain). *Zij een Germain priemgetal* (dat wil zeggen dat p priem is, en $q := 2p + 1$ is ook een priemgetal). *Neem aan dat*

$$x, y, z \in \mathbb{Z}_{>0} \quad \textit{zodanig dat} \quad x^p + y^p = z^p.$$

Dan is p een deler van xyz.

Dit is het zogenaamde "*eerste geval*" van FLT.
Opgave. *Bewijs dit voor het geval $p = 2$.* Vanaf nu zullen we veronderstellen dat p oneven is.
Het tweede geval behandelt de situatie dat p niet een deler is van xyz.
Deze stelling van Germain is een bijzonder geval van de stelling van Wiles, waarin FLT in volle algemeenheid bewezen (maar wel bijna 2 eeuwen later).

Zie b.v. [27], 3.2, of [84], Th. 65 in Ch III, voor een bewijs van (8.1). Overigens, de algemenere vorm die Germain bewees heeft tot gevolg datFLT bewezen werd voor alle p met $2 < p < 100$.

9 Een paar vermoedens

Overzicht:

Vermoeden	verwijzing
Mersenne priemgetallen	(9.3)
oneven perfecte getallen	(9.5)
Fermat priemgetallen	(9.7)
Goldbach	(9.8)
priem tweelingen	(9.10)
Polignac	(9.11)
FLT	(9.12)
Germain priemgetallen	(9.13)
ABC	(9.15)
Catalan	(9.16)
Mertens	(9.18)
Collatz	(9.19)
Congruente getallen	(9.20)
Riemann hypothese	
Hodge	
Birch & Swinnerton-Dyer	
Poincaré	
Serre	(9.21)

(9.1) De moderne wiskunde heeft een merkwaardige manier van werken ontwikkeld. Natuurlijk zijn er de bewezen stellingen en gevestigde theorieën. Dat arsenaal van kennis wordt gestaag uitgebreid. Maar er is een nieuwe werkmethode bijgekomen. We zien de enorme stimulerende kracht van *vermoedens*. Al werkend komt een wiskundige voor een moeilijk op te lossen probleem. Zonder een goede weg te vinden kan er wel een vraag worden gesteld, een probleem worden geopperd, uitgesproken hoe we verwachten dat de theorie eruit zal zien, en in het uiteindelijke geval formuleren we een vermoeden (in het Engels: "conjecture").

De wiskundige formuleert heel scherp wat reeds wel bewezen is, en wat nog weliswaar onbewezen is, maar toch waarschijnlijk wel zo in elkaar zit. De wiskundige is daar meestal veel precieser in dan bij voorbeeld wat in de natuurkunde gebruikelijk is (daar is het soms onduidelijk wat een bewezen feit is, wat een aanname is, wat een mogelijk theorie is, en nog meer van zulke begrippen).

We hebben gezien dat de wiskunde enorme impulsen krijgt door de goede vragen te stellen. Vroeger gebeurde dat niet zoveel in deze vorm. Wel werden er "programma's" op gesteld, vooruitlopend op mogelijke ontwikkelingen. Er werden wel een vragen gesteld, open problemen aangeroerd. Maar de enorme ontwikkeling in de richting van het formuleren van vermoedens is typisch iets van wiskunde na 1900.

In 1900 formuleerde David Hilbert op het International Congress of Mathematicians 23 problemen.

zie http://aleph0.clarku.edu/∼djoyce/hilbert/
Die bleken een enorme stimulans te zijn voor verder onderzoek. Ook deden we een verbluffende ontdekking. Hilbert gaf in veel gevallen aan welke problemen hij dacht dat ze erg moeilijk waren, en welke misschien wel snel opgelost zouden kunnen worden. In veel gevallen zat Hilbert er naast. En dat hebben we nog vaak gezien in de geschiedenis. Ikzelf zie de baanbrekende actie van Hilbert als richting gevend voor de 20-ste eeuwse wiskunde. Sommige van de problemen van Hilbert werden snel opgelost. Voor sommige ervan moest veel theorie ontwikkeld worden (en soms was het antwoord totaal verschillend van wat Hilbert verwacht had). En sommige van die problemen zijn nog steeds onopgelost, wachtend op die geniale inval, of op die ontwikkeling van de moderne wiskunde die toegang geeft tot die vraagstelling.

Het is, zelfs voor de begaafde en zeer rijpe wiskundige vaak niet mogelijk om aan te geven hoe moeilijk een probleem is. Ook weten we vaak niet uit welke hoek van de wiskunde een oplossing zou kunnen komen. Ikzelf zag daar een verbluffend voorbeeld van, een vermoeden op het grensvlak tussen getaltheorie en meetkunde, dat tenslotte opgelost werd met methoden uit de waarschijnlijkheidsrekening...

Het aantal vermoedens in de hedendaagse wiskunde is enorm. Er zijn grote collecties van problemen, die om een oplossing vragen. Het geeft richting aan het onderzoek (veel meer dan een preciese theorie kan doen). Het Clay Mathematics Institute formuleerde in 2000, een eeuw na de 23 problemen van Hilbert in 1900: "In order to celebrate mathematics in the new millennium, The Clay Mathematics Institute of Cambridge, Massachusetts (CMI) has named seven Prize Problems."
Zie http://www.claymath.org/millennium/ Een oplossing voor elk van deze problemen levert een miljoen dollar op.

Deze paragraaf zou vele honderden pagina's kunnen omvatten, als ik werkelijk een overzicht zou proberen te geven van vermoedens die nu in de moderne wiskunde in omloop zijn. Ook is het zo dat je voor sommige problemen veel voorkennis moet bezitten, wil je begrijpen wat het probleem is.

De meest in het oog springende van deze problemen is de "Riemann Hypothese", zie [76], zie het probleem 8 van met Hilbert, zie probleem 6 van het Clay Mathematics Institute. Er zijn veel boeken en artikelen die dit probleem uitvoerig toelichten. Er zijn ook veel resultaten beschreven die RH als hypothese aannemen, en die resultaten zijn nog onbewezen zolang de RH niet opgelost is; zie [26]. In het boek Marcus du Sautoy - *The music of the primes: Searching to solve the greatest mystery in mathematics* is er een beschrijving van dit probeem RH. - Helaas, om dat fascinerende probleem toe te lichten is er veel wiskundige voorkennis nodig. Daarom zal ik dat probleem niet uitleggen;
maar zie: http://www.claymath.org/millennium/Riemann_Hypothesis/
en verwijzingen daar genoemd.

Om toch een indruk te gevan de stimulerende invloed van vermoedens formuleer ik er een paar. Pas zei iemand tegen me: "Goede wiskunde kun je aan iemand op straat kunt uitleggen." Deze problemen zijn van die aard (of eventuele oplossingen dat ook zijn ?).

Een kleine waarschuwing. De onderstaande problemen zijn zo gemakkelijk te formuleren. Maar op de meeste van deze problemen hebben veel wiskundigen al hard en lang gewerkt. Dat een probleem gemakkelijk te formuleren is, zegt nog niet dat een mogelijke oplossing eenvoudig is. Dat hebben we gezien aan FLT, drie en een halve eeuw wiskundig ploeteren aan iets wat zo eenvoudig te formuleren is.....en de uiteindelijke oplossing is minder elementair dan de vraagstelling. Het is onwaarschijnlijk dat FLT via een elementair bewijs bevestigd kan worden. En het zellfde zou wel eens voor elk van de onderstaande problemen kunnen gelden. – Best leuk om even te proberen. Minder leuk om het als levenswerk te gaan zien.....

(9.2) Mersenne getallen. *Een getal van de vorm* $M_n := 2^n - 1$ *heet een Mersenne getal.*
We gaan zoeken naar Mersenne-priemgetallen.
Opmerking. We hebben gezien: *Als* M_n *een priemgetal is dan is* n *een priemgetal.* Zie (2.6)
Opmerking. De omkering geldt niet: M_{11} is niet een priemgetal want $M_{11} = 2047 = 23{\cdot}89$. Ga na: 47 is een deler van M_{23}.
Momenteel zijn er 46 Mersenne priemgetallen bekend. Er is een enorme "industrie" om Mersenne priemgetallen te vinden. Ervaring leert hoeveel er ongeveer moeten zijn, en waar ze mogelijk te vinden zijn. De theorie en de berekeningen nodig voor het vinden van Mersenne priemgetallen is formidabel. Voor informatie zie

http://primes.utm.edu/mersenne/
http://en.wikipedia.org/wiki/Mersenne_prime

(9.3) Vermoeden.$_{(?)}$ *Er zijn oneindig veel Mersenne priemgetallen.*(?)
Motivatie voor dit vermoeden: De "kans dat M_n een priemgetal is" is ongeveer $1/\log(M_n) \approx 1/(n\log(2))$. Het aantal Mersenne priemgetallen is "daarom" ongeveer

$$\sum_{n>0} 1/\log(M_n) \quad \approx \quad \frac{1}{\log(2)} \sum_{n>0} \frac{1}{n}.$$

We weten dat deze som divergeert. Dit geeft de suggestie dat er oneindig veel Mersenne priemgetallen zijn.

Het bevenstaande "bewijs" is onzin. Een gegeven getal M is wel of niet priem, en een uitspraak "de kans dat M priem is..." heeft geen enkele betekenis.

Voor wie nog niet overtuigd is: bewijs met de bovenstaande "redenering" dat er oneindig veel even priemgetallen zijn.

We hebben gezien dat voor elk Mersenne priemgetal $M_p = 2^p - 1$ het getal $N := 2^{p-1}{\cdot}(2^p - 1)$ een (even) perfect getal is, en dat omgekeerd alle *even* perfecte getallen op deze manier geconstrueerd worden, zie (2.3).

(9.4) Vraag. *Bestaat er een oneven perfect getal?*
We weten dat een dergelijk getal enorm groot is, als het bestaat (minstens 300 cijfers, tenminste een priemdeler van tenminste 20 cijfers). *Het lijkt daarom niet aan te raden met eenvoudige middelen een oneven perfect getal te gaan zoeken.* – In dit geval aarzel

ik om een vermoeden te formuleren. We hebben geen idee wat eruit komt. Het kan best dat er een heel groot getal is dat oneven en perfect is (waarom niet?). Het kan ook best zijn dat er een bewijs gevonden wordt dat een oneven perfect getal niet bestaat. Het bestaan van zulke getallen is bij mijn weten (nog) niet gekoppeld aan een ander verschijnsel in de wiskunde. – Het lijkt alsof we nog geen idee hebben waar te beginnen met een aanpak van dit probleem. Zie ook (2.11).

http://mathworld.wolfram.com/OddPerfectNumber.html

(9.5) Oneven perfecte getallen.
Verwachting.$_{(?)}$ *We verwachten dat er geen oneven perfect getal bestaat.*

Ik noem dit niet een vermoeden, omdat er weliswaar veel numerieke evendientie voor is, maar een structurele reden zien we nog steeds niet. Zie de disucssie verderop. Is dit een mooie en nuttige vraag? waar moeten we beginnnen? Vinden we misschien "toevallig" een oneven perfect getal? Of vinden we een mooie thorie die de verwachting ondersteunt of zelfs bewijst? Zie ook

(9.6) Fermat getallen. *Een getal van de vorm* $F_i := 2^{2^i} + 1, \quad i \in \mathbb{Z}_{\geq 0}$ *heet een Fermat getal.*
Voorbeelden. $F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537.$
Deze 5 getallen zijn priemgetallen. Fermat wist dit, en hij sprak de hoop uit dat alle Fermat getallen priem zouden zijn.

In 1732 bewees Euler: $F_5 = 2^{32} + 1 = 4294967297 = 641 \times 6700417.$

We kennen geen Fermat priemgetallen behalve de 5 bovenstaande. Van 238 verschilende Fermat getallen is bekend dat ze niet priem zijn. Het kleinste Fermat getal waarvan we niet weten (Januari 2009) of het een priemgetal is is F_{33}; dit is een getal met meer dan 2 miljard decimalen: $2^{33} \times {}^{10}\log(2) \approx 2585827972.$

(9.7) Fermat priemgetallen.
Vermoeden.$_{(?)}$ *Er zijn slechts eindig veel Fermat getallen die priem zijn.*

http://en.wikipedia.org/wiki/Fermat_number
http://www.prothsearch.net/fermat.html
http://mathworld.wolfram.com/FermatNumber.html

Zie ook (5.8).

Hoe komen we aan dergelijk vermoeden? Hier is een argument:
De "kans dat F_i priem is" is ongeveer $1/\log(F_i) = 1/(2^i \cdot \log(2))$. Het aantal Fermat priemgetallen is "daarom" ongeveer

$$\sum_{i \geq 0} \frac{1}{\log(F_i)} \quad \approx \quad \frac{1}{\log(2)} \sum_{i \geq 0} \frac{1}{2^i} \quad < \quad \frac{1}{\log(2)}.$$

Dit kan een aanduiding zijn dat het vermoeden juist is. Natuurlijk is dit argument als wismundig bewijs niet vele waard. Maar het geeft wel aan in welke richting we zouden moeten zoeken.

Overigens wees met dergelijke argumenten voorzichtig. Stel b.v. dat we niet op de hoogte zijn van (5.1). In onze onschuld zouden we proberen te bewijzen dat er veel getallen van de vorm $2^n + 1$ zijn die priem zijn. Met een “argument” als boven (bij de Mersenne getallen) gebruikt zouden we gaan denken dat er wellicht oneindig veel Fermat priemgetallen zouden kunnen zijn. Zulke “heuristiek” moeten we met grote voorzichtigheid en enige kennis van zaken hanteren. Zie:

http://primes.utm.edu/glossary/page.php?sort=Heuristic

Priemgetallen moet je vermenigvuldigen, niet optellen.
We zien veel interessante vragen, onopgeloste problemen als we sommen van priemgetallen gaan bekijken. Hier is het meest beroemde voorbeeld:

(9.8) Het Goldbach vermoeden.
Vermoeden.$_{(?)}$ *Zij $n = 2m \in \mathbb{Z}_{\geq 4}$ een even getal. Dan (?) zijn er priemgetallen p, en q zodanig dat $n = p + q$.*

Christian Goldbach schreef op 7 - VI - 1742 (in the Gregoriaanse kalender) een brief aan Euler, zie [29], waar hij dit probleem aan de orde stelde. Goldbach schreef: “Auf solche Weise will ich auch eine *conjecture* hazardieren ... dasz jede Zahl, die grösser ist als 2, ein *aggregatum trium numerorum primorum sei.*”
Commentaar:

Dit is de eerste plaats mij bekend in de wiskundige literatuur waar het woord *conjecture* op deze manier gebruikt wordt.

Goldbach beschouwde 1 ook als priemgetal, en in zijn terminologie zou elke $n \in \mathbb{Z}_{>2}$ de som moeten zijn van drie priemgetallen.

Leonhard Euler schreef terug op 30 - VI - 1742 dat hij deze uitspraak als “ein ganz gewissen Theorem” beschouwde, waarvoor Euler dan nog wel graag een bewijs zou willen zien.

Hoe moeten we dit probleem noemen? In het begin van de 20-ste eeuw sprak men van het “Goldbach-probleem”. In laat 20-ste eeuw gebruikte men “de Goldbach hypothese”. Tegenwoordig is gangbaar om te zeggen “het Goldbach vermoeden”.

Er is indrukwekkend veel numerieke evidentie. Momenteel is een bevestigend antwoord gevonden voor alle $n < 3 \times 10^{17}$ (Oliveira e Silva), 30-XII-2005;
zie http://mathworld.wolfram.com/GoldbachConjecture.html
Maar, zegt dit iets? Ik zie niet hoe we aan een abstract bewijs van het Goldbach Vermoeden zouden moeten beginnen. Het lijkt alsof dit nog een gesloten boek voor ons is. Wilt U een mooi boek hierover lezen? Zie [25]. Een fascinerende roman.

(9.9) “Het zwakke Goldbach Vermoeden”.$_{(?)}$ *Elk oneven getal $n = 2m+1 \in \mathbb{Z}_{\geq 9}$ is de som van drie oneven priemgetallen.*

We zeggen dat een tweetal getallen $(p, p + 2 = q)$ een priemtweeling is als zowel p als

$p + 2 = q$ priemgetallen zijn. Er zijn er ontzettend veel van bekend.

(9.10) Priemtweelingen.
Vermoeden.$_{(?)}$ *Het aantal priem-tweelingen is oneindig.*
Er is overweldigende numeriek evidentie hiervoor. Ook kunnen we een soort kansrekening opzetten, en als die zou kloppen dan is het vermoeden bewezen. Er zijn veel deelresultaten. Die "kansrekening" in dit geval geeft voorspellingen hoeveel priemtweelingen er beneden een gegeven grens zouden moeten zijn, en hoeveel er (ongeveer) op een gegeven interval zouden liggen. Die voorspellingen kloppen wonderwel met numeriek resultaten (noeste vlijt en rekenwerk). Dit geeft ons vertrouwen dat we in de goede richting zoeken. Maar een algemene theorie, of zelfs een algemeen vermoedde structuur die dit vermoeden zouden impliceren kennen we niet. Zie
http://primes.utm.edu/glossary/page.php?sort=TwinPrimeConjecture
http://mathworld.wolfram.com/TwinPrimes.html

(9.11) PolignacVermoeden.$_{(?)}$ *Voor elk even positief geheel getal n zijn er oneindig veel paren $(p, q = p + n)$ zodanig dat p en q priem en de tussenliggende getallen niet priem zijn.* M.a.w. priemgetal-gaten van lengte n komen oneindig vaak voor elk even positief geheel getal n.

Dit werd vermoed door Alphonse de Polignac in 1849, zie [71]. Het vermoeden is noch bewezen noch tegengesproken voor welke even $n \geq 2$ dan ook. Voor $n = 2$ komt er het priemtweelingen vermoeden. Voor $n = 4$ wordt dit wel het "priemneven probleem" genoemd. Voor $n = 6$ spreekt men wel van "sexy primes". Zie:
http://en.wikipedia.org/wiki/Polignac's_conjecture

Zie een serie voordrachten van fields medalist (2004) Terence Tao (google: Simons Lecture Tao). Daarin een fascinerend overzicht van methoden uit de waarschijnlijkheidsrekening toegepast in de getaltheorie. Met als prachtig resultaat ("er zijn willekeurig lange rekenkundige rijen van priemgetallen"):
Stelling (B. Green en T. Tao). *Voor elke $k \in \mathbb{Z}_{>0}$ zijn er oneindig veel paren $n, r \in \mathbb{Z}_{>0}$ zodanig dat de getallen $n, n + r, \cdots, n + ir, \cdots, n + kr$ allemaal priem zijn.*
Zie http://arxiv.org/abs/math.NT/0404188
Opmerking: dit lost het Priemtweelingen probleem en het Polignac probleem nog niet op.

(9.12) FLT.
Vermoeden.$_{(?!)}$

$$n \in \mathbb{Z}_{>3}, \quad x, y, z \in \mathbb{Z} \quad x^n + y^n = z^n \quad \stackrel{?}{\Longrightarrow} \quad xyz = 0.$$

Hier kan ik uren over praten (en dat deed ik ook in de HOVO-cursus in 2007). Dit vermoeden stond als stelling in de kantlijn opgetekend (waarschijnlijk in 1737) door Fermat. Eeuwen lang is hier aan gewerkt. Eerst was het een geïsoleerd probleem. Door suggesties van Hellegouarch en Frey, en werk van Serre en Ribet, bleek dit probleem een gevolg te zijn van een diep vermoeden op de grens van getaltheorie en meetkunde, het Shimura-Taniyama-Weil vermoeden. In 1995 lukte het Andrew Wiles een bewijs te geven van het geval van dit vermoeden dat nodig is om FLT te bewijzen; zie [99]. Zeer aanbevolen: het boek van Singh, zie [86] (en er zijn nog veel meer populaire en half-populaire boeken over dit prachtige onderwerp).

Dit vermoeden heeft de eeuwen dat het onopgelost was velen aangezet tot het ontwikkelen van nieuwe stukken wiskunde. In de 19-de eeuw werd een fundamenteel deel van de algebra ontwikkeld, en daarmee werden sommige gevallen bewezen. Het leek alsof de computer een rol ging spelen; met de opkomst van moderne rekentechnieken werden steeds meer gevallen bewezen (als ik het goed heb, werden alle gevallen met $2 < n < (3/2) \times 10^6$ zo bewezen). Totdat moderne methoden (Serre, Frey, Ribet, Wiles en vele anderen) een abstract bewijs gaven voor alle $n \geq 5$, gebaseerd op puur denkwerk (en $n = 4$, Fermat, $n = 3$, Euler waren reeds lang bekend). Een triomf van moderne wiskunde, die weer laat zien dat denken soms beter loont dan alleen maar rekenen.

(9.13) Germain priemgetallen.
Vermoeden.$_{(?)}$ *Het aantal Germain priemgetallen is oneindig.*
Overigens is ook onbekend of het aantal niet-Germain priemgetallen oneindig is (wel vermoed).
Toelichting: een priemgetal p heet een Germain priemgetal als ook $q := 2p + 1$ een priemgetal is.

Heuristiek zoals boven beschreven is bij Mersenne priemgetallen, Fermat priemgetallen en priemtweelingen kan ook hier beschouwd worden, en dit geeft als resultaat het bovenstaande vermoeden. Dit vermoeden is nog steeds onbewezen. Dezelfde heuristiek suggereert dat er oneindig veel priemgetallen zouden zijn die niet een Germain priemgetal zijn.

Hier volgt een vermoeden, eenvoudig te formuleren, met een enorme impact op de moderen getaltheorie.

(9.14) We bekijken drietallen $A, B, C \in \mathbb{Z}_0$ zodanig dat

$$A + B = C \quad \text{met} \quad \text{ggd}(A, B) = 1;$$

dan geldt ook $\text{ggd}(B, C) = 1 = \text{ggd}(C, A)$ (ga na). We definiëren het *radicaal* van dit drietal:

$$\text{Rad}(A, B, C) \quad := \quad \prod_{p|ABC} \quad p,$$

het product over alle priemgetallen (tot de macht 1) die ABC delen. We vragen ons af of een drietal kunnen vinden waarvoor C heel groot is en $\text{Rad}(A, B, C)$ heel klein. Dat kunnen we proberen te doen door ervoor te zorgen dat hoge machten van priemgetallen de drie getallen A, B en C delen. Dit "eenvoudige" probleem is moeilijker dan het op eerste gezicht lijkt. Als je dit probeert en A en B zijn van die vorm dan blijkt C geen hoge priem-machten te hebben.

(9.15) Het ABC-vermoeden (Masser, Oesterlé, 1985)
http://en.wikipedia.org/wiki/Abc_conjecture
http://www.math.unicaen.fr/~nitaj/abc.html

Vermoeden.$_{(?)}$ *Zij $\epsilon \in \mathbb{R}_{>0}$. Dan (?) is er een constante $\gamma = \gamma(\epsilon)$ met de eigenschap dat voor elk drietal (A, B, C) als boven geldt:*

$$C < \gamma(\epsilon) \times (\mathrm{Rad}(A, B, C))^{1+\epsilon}.$$

H. W. Lenstra: "We kunnen dit ook wel het XYZ-vermoeden, of het KLM-vermoeden noemen."

Hier is een eenvoudiger vorm, een variant van dit vermoeden. We kiezen $\beta \in \mathbb{R}_{>1}$.
Uitspraak.

$$(ABC)_\beta \text{ } \textit{Voor elk drietal als boven geldt } C < (\mathrm{Rad}(A, B, C))^\beta.$$

Vermoeden. *Er bestaat een $\beta \in \mathbb{R}_{>1}$ zodanig dat $(ABC)_\beta$ juist is.*

Notatie. Schrijf $\alpha(A, B, C) := \log(C)/\log(\mathrm{Rad}(A, B, C))$. We proberen te zien of de waarden van $\alpha(A, B, C)$ begrensd als we alle toegestane drietallen beschouwen.
Een voorbeeld:

$$2 + 3^{10} \cdot 10^9 = 23^5; \quad \text{Eric Reyssat, 1987} \quad \alpha \approx 1.62991.$$

Zie ($\alpha =$ "quality")
http://www.math.leidenuniv.nl/ desmit/abc/index.php?sort=1
voor nog veel meer voorbeelden. Momenteel is dit het drietal met de hoogste α. Dat impliceert:

Eerste verrassing. *We kennen geen tegenvoorbeeld tegen $(ABC)_2$.*

Tweede verrassing. *Zij $n \in \mathbb{Z}$; dan geldt:*

$$n > 3{\cdot}\beta, \quad (ABC)_\beta \quad \Longrightarrow \quad \mathrm{FLT}_n.$$

Bewijs. Neem aan dat $a, b, c, n \in \mathbb{Z}_{>0}$ met $a^n + b^n = c^n$. Voor het drietal

$$A = a^n, \ B = b^n, \ C = c^n \quad \text{geldt} \quad \mathrm{Rad}(A, B, C) = \mathrm{Rad}(a, b, c) < c^3.$$

Als $(ABC)_\beta$ geldt, weten we dat voor elke keuze, dus zeker voor deze keuze

$$c^n = C < (\mathrm{Rad}(A, B, C))^\beta < c^{3\cdot\beta}.$$

De tegenspraak met $n > 3{\cdot}\beta$ (merk op dat $c > 1$) bewijst de bewering. QED

Zie ook de Nederlandse versie van [86] pag. 310.

(9.16) Catalan.
We beschouwen x^a een "pure macht", waar x en a gehele getallen zijn die minstens 2 zijn. Kunnen we dit zo kiezen dat dan ook $x^a + 1$ een pure macht is? Kwadraten verschillen niet 1. Maar het zo kunnen zijn dat een kwadraat en een derde-macht 1 verschillen , of .. ?? Eugne Charles Catalan vermoedde in 1844:

Vermoeden.$_{(?)}$

$$x, y, a, b \in \mathbb{Z}_{>1} \quad x^a + 1 = y^b \quad \overset{?}{\Longrightarrow} \quad x^a = 8, \quad y^b = 9.$$

Dit vermoeden heeft een rijk verleden. Van de vele deelresultaten vermeld ik de spectaculaire stelling van Tijdeman; hij bewees dat elke oplossing van de Catalan vergelijking gelegen is beneden een expliciet gegeven grens; dit bewijst dat het aantal oplossingen van de Catalan vergelijking eindig is. Zijn we dan klaar? Die grens was zo ontzettend groot, dat het rekenwerk om het vermoeden ook echt te bewijzen ondoenlijk was. Wel werd die grens steeds iets naar beneden gebracht, maar het bleef nog steed buiten het bereik van zelfs de snelste computers. De volgende verrassing was dat Preda Mihăilescu in 2002 dit vermoeden bewees, zie [59]; bovendien bleek het bewijs een mooie combinatie te zijn van methoden die allang bekend waren. Hier heeft het bewijs van een vermoeden dus niet een stroom aan nieuwe technieken nodig.

http://www.math.leidenuniv.nl/ jdaems/scriptie/Catalan.pdf
http://en.wikipedia.org/wiki/Tijdeman
http://en.wikipedia.org/wiki/Mih

Opmerking. Voor $8 + 1 = 9$ krijgen we $\mathrm{Rad}(8, 1, 9) = 6$ en $9 = 6^\alpha$ geeft $\alpha \approx 1.226294386$. Welke vorm van ABC hebben we nodig om het Catalan vermoeden te bewijzen?

(9.17) Om het Mertens vermoeden te formuleren hebben we enig notatie nodig. Voor $n \in \mathbb{Z}_{>0}$ defniëren we $\mu(n)$ de "Möbius functie" (de functie geïntroduceerd door in 1832 en de notatie $\mu(n)$ gebruikt door Mertens in 1874)

we schrijven $\mu(1) = 1$,

als n deelbaar is door een kwadraat groter dan 1, dan is $\mu(n) = 0$,

en als n het product is van k onderling verschillende priemfatoren, dan is $\mu(n) = (-1)^k$.

We zien dat de waarde vaak $+1$ is, soms 0 en soms -1. Bovendien lijkt het dat de waarde $+1$ vaker voorkomt dan de waarde -1 (eerst komen 2 en 3, en dan pas 6 ... wat een gammel argument). Wat zou er gebeuren als die waarden optellen?

$$M(n) := \sum_{i=1}^{i=n} \mu(i)$$

Als we hiermee experimenteren, dan zien we dat de waarde van $M(i)$ voor groeiende i dicht bij 0 blijft.
Suggestie: maak een lijst van positieve gehele getallen, met daarachter de waarden van $\mu(n)$, en daarachter de waarden van $M(n)$. Zien we die waarden van $M(n)$ snel oplopen? of juist heel laag blijven? Het volgende vermoeden lijkt heel plausibel.

(9.18) Vermoeden.$_{(?)}$ Mertens, 1897.

$$\forall n > 0 \quad M(n) < \sqrt{n}.$$

Dit lijkt redelijk. Mertens verifiëerde het vermoeden voor $n < 10000$ in 1897. Sterneck bewees in 1912 dat het vermoeden juist is voor $n < 500000$. Dat is toch enorme numerieke evidentie ?! Bovendien werd bewezen dat dit vermoeden het beroemde vermoeden van Riemann impliceert. We leken dicht bij en oplossing van allebei.

Groot was de verrassing toen Odlyzko en Te Riele in 1985 bewezen dat het Mertens vermoeden onjuist was. Ze gaven weliswaar geen grens aan waar het ongelijkteken omslaat, maar dat dit bij heel grote getallen zou moeten gebeuren was wel duidelijk; zij dachten dat dat pas gebeurt ergens na $n = 10^{30}$. Pintz bewees in 1987 dat er een tegenvoorbeeld tegen het Mertens vermoeden is voor een n met $n < e^{3.21\times10^{64}}$ (een vreselijk groot getal). – We zien hoe voorzichtig we moeten zijn met "numerieke evidentie". Zie ook het Pólya vermoeden, zie ook het getal van Skewes:

http://en.wikipedia.org/wiki/P%C3%B3lya_conjecture
http://en.wikipedia.org/wiki/Skewes%27_number

allemaal voorbeelden waar numerieke evidentie zelfs voor heel grote getallen het verkeerde resultaat suggereren.

Het Mertens vermoeden is onjuist. Maar dit bewijst nog niet dat het Riemann vermoedendan ook onjuist is ?!

http://mathworld.wolfram.com/MertensConjecture.html
http://en.wikipedia.org/wiki/Mertens_conjecture
http://www.dtc.umn.edu/~odlyzko/doc/arch/mertens.disproof.pdf
http://www.math.tu-berlin.de/~kant/ants/Proceedings/te_riele/te_riele_talk.pdf

(9.19) Collatz rijen. Begint met $x_0 \in \mathbb{Z}_{>0}$ en maak een rij $x_0, x_1, \cdots$ volgens de regel:

als x_i oneven is, dan is $x_{i+1} = 3x_i + 1$;
als x_i even is, dan is $x_{i+1} = x_i/2$.

Verwachting (Collatz). *Voor elke begin waarde $x_0 \in \mathbb{Z}_{>0}$ is er een $j \in \mathbb{Z}\geq 0$ zo dat $x_j = 1$.*
(Waarom ik hier "verwachting" en niet "vermoeden' schrijf? zie (9.22).)

Voorbeelden: $6, 3, 10, 5, 16, 8, 4, 2, 1$ (en verder: $4, 2, 1, 4, 2, 1 \cdots$).
$11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, \cdots$.
Het Collatz vermoeden is bewezen voor alle beginwarden beneden $20\times2^{58} \approx 5.764\times10^{18}$. Met $x_0 = 27$ komen er 111 stappen, we komen boven $9,000$, maar uiteindelijk kom 1 in deze Collatz-rij voor; deze rij vinden we op de site:

http://en.wikipedia.org/wiki/Collatz_conjecture

Op de volgende sites wordt een Collatz rij uitgerekend bij een ingetypt begingetal:

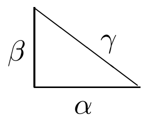
http://www.numbertheory.org/php/collatz.php
http://www.freemotion.nl/reken/collatz.php

Op de volgende site, op pag. 14 vinden we een paar experimentele gegevens. Bij voorbeeld: begin met 77671, getallen in de Collatz-rij komt boven een miljard, en na 231 stappen komen we tenslotte bij 1:

http://www.logika.umk.pl/llp/141/jpvb.pdf

Dit vermoeden is onbeslist. We hebben eerder al gezien dat we voorzichtig moeten zijn met numeriek evidentie. Ik zie voorlopig nog geen methode die echt toegang geeft tot dit probleem.

(9.20) Congruente getallen.
Definitie. Een positief geheel getal N heet een *congruent getal*, afgekort CG, als er een rechthoekige driehoek bestaat met lengtes van zijden in $\mathbb{Q}_{>0}$ en met oppervlak gelijk aan $N \in \mathbb{Z}$.
Noem de lengtes van de zijden $\alpha, \beta, \gamma \in \mathbb{Q}$; met behulp van de stelling van Pythagoras zien we:



$\alpha \cdot \beta/2 = N,$
$\alpha^2 + \beta^2 = \gamma^2;$
een voorbeeld is: $\alpha = 9/6, \quad \beta = 40/6, \quad \gamma = 41/6, \quad N = 5.$

Eenvoudig in te zien:
$n = 6$ is een CG, want $3^2 + 4^2 = 5^2$,
$n = 5$ is een CG, want $(9/6)^2 + (40/6)^2 = (41/6)^2$.

De vraag welke gehele getallen een CG zijn werd gevraagd in een anoniem 10-de eeuws Arabisch manuscript, zie [1]. Daarna veelvuldig bestudeerd door Fibonacci, Fermat, en vele anderen. Echter de vraag hoe te bepalen of een gegeven geheel getale een CG is, is 10 eeuwen later nog niet bevredigend opgelost.

Hier is een niet eenvoudig geval:
$n = 1$ is niet een CG;
dit was eeuwen lang een open probleem, en verkeerder oplossingen werden aangekondigd. Dit probleem pas door het genie Fermat opgelost. Zie [20], p. 462; zie [16], p. 10.

Bij gegeven getal n, als we weten dat het congruent is, dan is de omvang van de teller en noemer van α, β en γ in de definitie, nodig om te bewijzen dat het getal congruent is, niet te voorspellen uit de grootte van n.

In 1977 (Coates en Wiles) en 1983 (Tunnell) zagen we dat we effectief kunnen bepalen welke getallen congruent zijn indien het vermoeden van Birch en Swinnerton-Dyer juist is. We hebben nu een vermoeden wat dit effectieve critrium zou kunnen zijn. Zie: [15], [93], zie [51], pag. 221, zie [66], [67]

(9.21) Diverse vermoedens. In deze paragraaf heb ik een aantal vermoedens vermeld. Maar veel meer is onbesproken gelaten. In mijn selectie vban de vermoedens hierboven genoemd heb ik vooral gelet op de eigenschap van een probleem of je met eenvoudige middelen kunt aangeven wat er bewezen zou moeten worden. Daarbij zijn juist de belangrijkste vermoedens onbesproken gebleven. Bij voorbeeld de Clay Millenium Problems, zie:

http://www.claymath.org/millennium/

Helaas vallen onder andere buiten het bestek van elementaire wiskunde:

- **De Riemann Hypothese.** Zie

  http://en.wikipedia.org/wiki/Riemann_hypothesis

  http://modular.math.washington.edu/edu/2007/simuw07/misc/Official_Problem_Description.pdf

  Er zijn vele boeken over dit onderwerp geschreven. Zie [26]. Zie bv. [81]. De numeriek evidentie overweldigend. De gevolgen voor de wiskunde (zouden) heel groot zijn; nu al zijn er veel stellingen bewezen onder "aanname van de RH". Een heel goed leesbare elementaire inleiding:
  R. van der Veen & J. van de Craats
  De Riemann-Hypothese, een miljoenenprobleem.
  Lesteksten bij de webklas Wiskunde - najaar 2006.

  http://staff.science.uva.nl/∼craats/RH.pdf

- **De vermoedens van Birch en Swinnerton-Dyer.** Zij kwamen op het idee om het "aantal" rationale punten op een elliptische kromme in verband te brengen met het gedrag van een analytische functie. Zij rekenden (op een computer) veel speciale gevallen door, en vonden na een paar benaderingen een formulering die sindsdien niet tegengesproken (maar ook nog niet bewezen) is. Zie [8]. Zie:

  http://planetmath.org/encyclopedia/BirchAndSwinnertonDyerConjecture.html

  http://www.claymath.org/millennium/Birch_and_Swinnerton-Dyer_Conjecture/BSD.pdf

- **Het Hodge vermoeden.** Deelvariëteiten geven bepaalde klassen in een groep gehecht aan de omringende variëteit. Kun je omgekeerd het bestaan van deelvariëteiten afleiden uit het bestaan van bepaalde klassen? Hodge formuleerde dit (later gepreciseerd door Grothendieck). Zie:

  http://en.wikipedia.org/wiki/Hodge_conjecture

- **Het Poincaré vermoeden.** Dit was een van de belangrijkste vragen in de topologie. Een lus die op een boloppervlak getekend is kan samengetrokken worden; een boloppervlak noemen we een 2-sfeer. Is een 3-voud met deze eigenschap een 3-sfeer? Dat is het vermoeden. Het werd bewezen door Grigori Perelman in 2003; daarvoor kreeg hij de Fields medaille (die hij niet accepteerde; dit is de "Nobel prijs voor de wiskunde"), en nog veel meer roem. Na deze prachtige prestatie heeft Perelman, naar het schijnt, de wiskunde verlaten:

  http://en.wikipedia.org/wiki/Grigori_Perelman

- **Het Serre-vermoeden.** Dit vermoeden is te vinden in [82]. Dit vermoeden is sterk genoeg om FLT als gevolg te hebben. Het legt veel bloot van een diepere structuur op het grensvlak tussen de getaltheori, de algebra an de analyse. Dit is ongetwijfeld een onderwerp wqaar de komende jaren nog veel ontwikkeling in zal te zien zijn. Ondertussen is dit vermoeden bewezen. Een formulering van en een schets van het bewijs is te vinden op:

http://modular.fas.harvard.edu/papers/serre/ribet-stein.pdf

Opmerking. Vaak zetten we bij een resultaat in de wiskunde een naam. Maar laten we wel goed realiseren dat heel vaak werk gebaseerd is op ideën en deelresultaten van vele anderen. Bij elke belangrijk resultaat hierboven kun je een lange lijst van namen geven van mensen die bijgedragen hebben aan de ontwikkeling van dat resultaat.

(9.22) Een discussie. Het centrale thema van deze reeks voordrachten is het beang van vermoedens in het ontwikkelen van wiskundige ideeën. Maar soms wordt maar al te gauw iets tot een "Conjecture" (vermoeden) gepromoveerd. Daarom stel ik de volgende hierachie voor:

- **Vraag.** In de wiskunde kunnen we een vraag stelen. Dat is vaak het begin van een interessante onwikkeling.
- **Probleem.** Als we een vraag een tijdje bestudeerd hebben, en er komt meer structuur in onze gedachten daarover, dan kunnen we die vraag vaak preciseren tot een probleem.
- **Verwachting.** Als we dan beginnnen in te zien, door numeriek evidentie, doordat veel gevallen kloppen, doordat het er "zo mooi uitziet", of hoe dan ook, dan kunnen we verwachten dat het probleem een bepaalde oplossing heeft. Ik ben ervoor om alles wat niet aan criteria voldoet, zoals hier beneden zal worden uiteengezet, nog niet een vermoeden te noemen.
- **Vermoeden.** Als we sterke aanwijzingen hebben dat iets waar zou kunnen zijn, maar nog geen bewijs, dan kunnen we dit formuleren als vermoeden. Ik vind dat daar dan aan tenminste één van de volgende voorwaarden moet zijn voldaan:

  1. *Structurele evidentie.* Soms ontdekken we dat een vermoeden een bijzonder geval is van een veel algemenere structuur, die misschien nog niet bewezen is. We zagen dat bij voorbeeld bij FLT, eeuwen lang een geïsoleerd probleem, maarvanaf 1985 in verband gebracht met een veel algemener vermoeden.
  2. *Numeriek evidentie.* Hier moeten we voorzichtig mee zijn (beoordeling hangt heel erg af van de expertise, van de ervaring die iemand heeft die ermee omgaat). We hebben voorbeelden gezien waar "heel veel gevallen reeds bewezen waren", en waar de algemene uitspraak fout is. Wiskundigen zijn er sterk in om onbewezen vermoedens en ware uitspraken van elkaar te scheiden!
  3. *Structuur in bijzondere gevallen.* Soms bewijzen we een algemene uitspraak in een aantal belangrijke speciale gevallen. Intuïtief voelen we dat als het in "deze" gevallen goed gaat, dat het dan ook algemeen wel zo zou moeten zijn.

4. *Analogie.* Vaak zijn er twee wiskundige situaties die als twee druppels water op elkaar lijken, en waar in de ene theorie een uitspsraak waar blijkt te zijn; dan zijn we geneigd om de "vertaling" van die bewering naar de andere situatie als vermoeden te formuleren.
   Een voorbeeld: André Weil formuleerde in 1940 $\sim$ 1946 een vermoeden dat geheel parallel loopt aan het Riemann Vermoeden. Het vermoeden van Weil werd in 1972 bewezen door Deligne. Dit is een sterke aanwijzing voor ons dat het oorspronkelijke vermoeden vanRiemann waar zou kunnen zijn. Overigens bij "analogie" denk ik aan het vertalen van een formulering, zonder dat de bewijsmethoden ook vertaald zouden kunnen worden (als dat wel kan, dan ben je klaar). (Overigens, voor de Weil vermoedens had André Weil heel sterke "Structurele evidentie".)
5. *Elegantie.* Wiskundigen hebben een hoog ontwikkeld gevoel voor schoonheid. Er zijn van die uitspraken waar je hij voelt: "als iets waar zou zijn, dan moet het zó in elkaar zitten".

Overigens, geen enkel van deze voorwaarden biedt garantie voor uiteindelijk succes, allicht niet.

(9.23) Nog een waarschuwing tegen "numeriek evidentie". We proberen de vergelijking

$$X^2 - 1141{\cdot}Y^2 = 1$$

op te lossen met $x, y \in \mathbb{Z}_{>0}$. Is het nuttig om "zo maar eens wat te proberen" ? Het blijkt dat er geen oplossing is waarvoor $0 < y < 10^{25}$. Maar we weten uit de theorie van de Fermat-Pell vergelijking dat er wel degelijk oplossingen zijn (en zelfs oneindig veel). De kleinste y waarvoor een oplossing bestaat heeft 26 cijfers. – Soms horen we wel eens dat we wiskundig onderzoek kunnen vervangen door het installeren van voldoend sterke computers; die rekenen nu nog aan deze vergelijking, terwijl een student op een college elementaire getaltheorie leert dat deze vergelijking wel degelijk oplossingen heeft (en ook leert hoe je ze effectief moet vinden).

10 Appendix A: De kalender

(10.1) Het doel van de **"kalendermethode"**: geef een datum, en bereken daaruit op welke dag van de week die valt (of viel). Het blijkt dat die methode gemakkelijk te gebruiken en eenvoudig te onthouden is. Ik gebruik deze methode vaak.

Eerst enkele bekende begrippen. We zullen de maanden nummeren door: januari = I, februari = II, maart = III, $\cdots$, oktober = X, november = XI, december = XII.

Dit doe ik om verwarring te voorkomen. In het nederlands zeggen we "3 januari", in het engels "January 3", wat wordt er bedoeld met "03-01-1993", is dat 3 januari of 1 maart? Op formulieren schrijven we dan meestal "03-01-1993", en we bedoelen 3 januari, ik geef de voorkeur aan "03-I-1993". Zo is 4-III = 3 maart (de dag dat deze cursus in 2009 begint). Dat is een woensdag kunnen we die dag snel bepalen?

We weten dat het aantal dagen van de verschillende maanden is:
I (31), **II (28 of 29)**, III (31), IV (30), V (31), VI (30),
VII (31), VIII (31), IX (30), X (31), XI (30), XII (31).

Wat is de reden van dat springen van het aantal dagen van februari? De aarde loopt niet precies in 365 dagen om de zon heen, maar we willen wel dat Kerstmis ergens in de winter valt, en dat juli ergens in de zomer valt, en dat het zo blijft in de loop van de eeuwen. De *gregoriaanse kalender* corrigeert dit door de meeste jaren uit 365 dagen te laten bestaan, maar in sommige andere jaren gaat er één dag meer in een kalenderjaar:

Een **schrikkeljaar** is een jaar waarin februari 29 dagen heeft;
in alle andere jaren heeft februari 28 dagen.

De jaren $\cdots$, 2004, 2008, 2012, $\cdots$ zijn schrikkeljaren
(het jaartal is wél deelbaar door 4),
de jaren $\cdots$ 2001, 2002, 2003, 2005, $\cdots$ zijn niet schrikkeljaren.
(het jaartal is níét deelbaar door 4)
Verder is er de afspraak: 1700, 1800, 1900, 2100 zijn niet schrikkeljaren,
en 1600, 2000, 2400 zijn wél schrikkeljaren
(d.w.z. als een getal n deelbaar is door 4, dan is n $\times$ 100 wel een schrikkeljaar, als n niet deelbaar is door 4, dan is het niet een schrikkeljaar). Ja, het is een beetje gecompliceerd, maar zo bereiken we dat voorlopig het gemiddeld aantal dagen in een jaar met grote nauwkeurigheid gelijk is aan de omloopstijd van de aarde om de zon.

(10.2) **Opgave.** 3 maart 1788 en 3 maart 1788+28 vallen op dezelfde dag, maar 3 maart 1888 en 3 maart 1888+28 vallen niet op dezelfde dag. (Algemeen: periodiciteit van 28 jaar als in die periode niet een eeuwjaar bevat, want $7 \times 366 + 21 \times 365$ is deelbaar door 7, allicht).
Opgave. Bewijs dat het aantal dagen in een periode van precies 400 jaar deelbaar is door 7 (en concludeer: 3 maart 1788 en 3 maart 2188 vallen op dezelfde dag van de week).
Opgave. Bereken in een periode van 400 jaar voor getal $\{1, 2, \cdots, 30, 31\}$ hoe vaak dat

getal voorkomt op welke dag van de week. Concludeer dat "vrijdag de 13-de" de grootste frequentie heeft! (Een hele rekenpartij.)

(10.3) De jaardag. Om deze kalendermethode te gaan gebruiken definiëren we de **jaardag** van een zeker jaar: het is de dag van de week waarop de laatste dag van februari valt in dat jaar.
Voorbeeld: In 1993 valt 1 maart op een maandag (het is níét een schrikkeljaar, februari 1993 heeft daarom 28 dagen, 28-II-1993 is een zondag), en we schrijven:

$$\text{jd}(1993) = \text{zondag} = \text{zo}.$$

Kijken we b.v. naar 1992, dan is 1-III-1992 een zondag (1992 is wél een schrikkeljaar, en 29-II-1992 valt op een zaterdag), we schrijven:

$$\text{jd}(1992) = \text{zaterdag} = \text{za}.$$

Natuuurlijk kunnen we zodra we één jaardag weten, alle andere berekenen (merk op: van 2001 naar 2002 schuift de jaardag een naar voren, van 2003 naar 2004 schuift de jaardag 2 naar voren). Het is wel handig om een paar gegevens in een tabel te hebben:

jaartal = n	jaardag= jd(n)
1700	zo
1800	vrij
1900	woe
2000	di
···	···
1980	vrij
1990	woe
1991	do
1992	za
1993	zo
1994	ma
···	···
1999	zo
2000	di
2001	woe
2002	do
2003	vrij
2004	zo
2005	ma
2006	di
2007	woe
2008	vrij
2009	zat
2010	zo
···	··· etc.

Hoe berekenen we uit jd(1900)=woe de jaardag van bv. 1978? Als we van 1900 naar 1978 gaan, dan is dat 78 jaren verder, en we passeren van 1901 t/m 1978 precies 19 schrikkeljaren. De jaardag schuift dus 78+19 dagen op, en schuift daarom van een woensdag naar een dinsdag.
Oefenen: jd(1800)=vrij, wat is jd(1888)?

(10.4) Verder onthouden we voor elke maand een getal:

III = maart		7 = 3+4
IV = april	4	
V = mei		9 = 5+4
VI = juni	6	
VII = juli		11 = 7+4
VIII = augustus	8	
IX = september		5 = 9-4
X = oktober	10	
XI = november		7 = 11-4
XII = december	12	
II = februari		laatste
I = januari		laatste (+1 als s.)

Wat is de betekenis van deze getallen? In de tabel staat achter maart het getal 7, en daarmee bedoelen we dat 7 maart op dezelfde dag valt als de laatste dag van februari, dus 7 maart valt op de jaardag:

$$\text{dag(7-III-2024)} = \text{jd(2024)}.$$

Idem voor 4 april, die valt ook op de jaardag, evenzo voor 9 mei en zo gaan we door. De reden dat we het zo doen, is dat dit gemakkelijk te onthouden is:

- voor de "even"maanden april, $\cdots$, december nemen we gewoon het rangnummer van de maand,
- voor maart, mei, juli tellen we 4 op bij het rangnumer,
- voor september en november trekken we er 4 vanaf.

(10.5) We passen de kalender-methode toe:
Voorbeeld. Neem 13 oktober 1993, de eerste tabel geeft: jd(1993) =zo, dus de laatste dag van februari 1993 is een zondag, evenzo is 10-X-1993 een zondag (gebruik de tweede tabel), en we zien direct dat 13-X-1993 op een woensdag valt.
Voorbeeld. Op welke dag viel StNicolaas in 1979? Eerste tabel: jd(1979) = woe, gebruik tweede tabel, en concludeer dat 12-XII-1979 een woensdag was.
Voorbeelden. dag(5-V-1945) = za; jd(1940) = jd(1968) = jd(1996) = do, en we zien dat dag(10-V-1940) = vrij.
Voorbeeld. Neem 14-II-1992, merk op dat 1992 een schrikkeljaar is, uit de tabel zien we daarom dat dag(29-II-1992)= za, en we concluderen dag(14-II-1992)= vrij.

Evenzo proberen we 5-I-1993: we zien dag(28-II-1993)= zo = dag(31-I-1993), en concluderen: dag(5-I-1993) = di. Oefenen!
Opgave: Bereken de dag van Uw eigen verjaardag.
Strikvraag: Op welke dag van de week viel 29-II-1978?

We weten: jd(2009)=za; omdat 4=III vier dagen later is dan de aatste dag in februari zien we: dag(4-III-2009) = woe.

(10.6) **Opgave.** Hoe heet de dag 5-IX-1944 ?

(10.7) **Opmerking.** De kalender die we nu gebruiken werd in 1582 ingevoerd door Paus Gregorius XIII; we noemen deze jaartelling de *gregoriaanse kalender*. Daarvóór gebruikte men de *juliaanse kalender*, ingevoerd door Julius Caesar in 46 voor Chr. Die jaartelling had een kleine onnauwkeurigheid, die in de loop van de jaren tot steeds grote afwijkingen aanleiding gaf. De datum 5-X-1582 (juliaans) werd gelijk gesteld aan 15-X-1582 (gregoriaans).

Het verschil tussen de twee jaartellingen: 1300, 1400, 1500, 1700, 1800, 1900, 2100, etc. zijn in de juliaanse wél in de gregoriaanse kalender níét een schrikkeljaar. Dit verschil van 3 dagen per 400 jaar bleek net voldoende om de nodige correctie uit te voeren.

NB Er zijn ook heel andere jaartellingen. De joodse, de islamitische, de japanse jaartelling zijn daar voorbeelden van, die nu nog steeds intensief (naast ”onze”jaartelling) gebruik worden.

NB Het is niet zo dat in 1582 de gregoriaanse kalender overal direct ingevoerd werd. Hoe dat gebeurde is een ingewikkelde geschiedenis (zie bv. W. E. van Wijk - Onze kalender. Wereld-Bibliotheek, Amsterdam, 1955). Het is mij b.v. niet duidelijk in welke kalender

de geboortedag van Johann Sebastian Bach 21-III-1685 gerekend is (data ná 1776 zijn in heel **Duitsland** in de gregoriaanse kalender, tussen 1582 en 1776 kan dat van plaats tot plaats verschillen).

1582: gregoriaanse kalender in **Frankrijk** en **Spanje**,
1752: **Engeland** en de kolonies daarvan,
Rusland: na de revolutie van 1917.

De bovenstaande methode is afkomstig van J. H. Conway. Zie ook H. M. Stark - An introduction to number theory. Markham, 1970, pp. 113 - 116.

(10.8) **Oplossing van** Opgave (10.6). De vraag is niet wat dag(5-IX-1944) is. Maar dat kunen we wel eerst uitrekenen: jd(1944)= jd(1900) + 44 + 11 = woe + 55 = di. Dus is dag(5-IX-1944) = di. Dan komen we misschien op de oplossing: die dag heette “dolle dinsdag”. Zie

http://nl.wikipedia.org/wiki/Dolle_Dinsdag

11 Appendix B: Het 15-spel

(11.1) Men zegt dat de grote puzzel-expert Sam Loyd (soms gespeld als Sam Lloyd, of Samuel Loyd) in 1878 een puzzel maakte die bestaat uit een rechthoekige doos van afmeting 4×4 met daarin 15 blokjes genummerd van 1 tot en met 15. Zie [S-Nl-FLT] pag. 154. We kunnen blokjes horizontaal of verticaal schuiven naar het lege vakje. Uitgaande van een beginsituatie is de opgave door schuiven de **standaard-situatie** te bereiken:

1	**2**	**3**	**4**
5	**6**	**7**	**8**
9	**10**	**11**	**12**
13	**14**	**15**	**L**

De beginsituatie die Loyd als uitdaging gaf bestond uit: alle blokjes $1, \cdots, 13$ op hun plaats, en dan daarna 15 en 14 (verkeerd om). Het lijkt een eenvoudig opgave. Een beetje schuiven, en dan de uitgelofde prijs van $ 1000 incasseeren. Loyd schrijft daarover in "Sam Loyd's Cyclopaedia of 5000 Puzzles, Tricks and Conundrums", gepubliceerd in 1914 door zijn zoon (die ook Sam Loyd heette):

"Older inhabitants of Puzzleland will remember how in the seventies I drove the entire world crazy with a little box of movable blocks which became known as the "14-15 Puzzle". The fifteen blocks were arranged in the square box in rectangular order, but with the 14 and 15 reversed. The puzzle consisted of moving the blocks about, one at a time, to bring them back to the present position in every respect except that the error in the 14 and 15 was corrected.

A prize of $1000, offered for the first correct solution to the problem, has never been claimed, although there are thousands of persons who say they have performed the required feat.

People became infatuated with the puzzle and ludicrous tales are told of shopkeepers who neglected to open their stores; of a distinguished clergyman who stood under a street lamp all through a wintry night trying to recall the way he had performed the feat. The mysterious feature of the puzzle is that none seem able to remember the sequence of moves whereby they feel sure they have succeeded in solving the puzzle. Pilots are said to have wrecked their ships, and engineers rush their trains past stations. A famous Baltimore editor tells how he went for his noon lunch and was discovered by frantic staff long past midnight pushing little pieces of pie around on a plate! Farmers are known to have deserted their ploughs ... "

Opmerking. Het is mogelijk dat Loyd deze puzzel overnam van een eerdere bron, zie: Jerry Slocum and Dic Sonneveld - "The 15 Puzzle"(ISBN 1-890980-15-3): "Sam Loyd

heeft de 15 puzzel niet uitgevonden en heeft ook niets te maken met het populariseren van deze puzzel. De puzzel gekte die ontstond rond de 15 Puzzle begon in januari 1880 in Amerika en in april in Europa. De gekte eindigde in juli 1880 en Sam Loyds eerste artikel over de 15 puzzel werd pas 16 jaar later gepubliceerd, in januari 1896. Loyd beweerde voor het eerst in 1891 dat hij de puzzel heeft uitgevonden, en hij hield deze leugen vol tot aan zijn dood 20 jaar later. De echte uitvinder was Noyes Chapman, een postbeambte uit New York, die al een patent aanvroeg in maart 1880."
Zie http://bd.thrijswijk.nl/15puzzle/15puzznl.htm

(11.2) Is de puzzel wel zo eenvoudig? Een paar blokjes in een doosje. Met wat schuiven kun je toch alle situaties analyseren?
Opgave. Onderstel dat iemand elke seconde één situatie van het 15 spel realiseert, 12 uur per dag, 365 dagen per jaar. Hoeveel jaar zou die persoon dan bezig zijn?

Het blijkt dat "even proberen" niet zo eenvoudig is. Het zal ook blijken dat de duivelse opgave die Sam Loyd voorstelde geen oplossing heeft. In plaats van "domweg proberen" gaan we nadenken.

(11.3) De constructie van een invariant. Zij S een situatie, d.w.z. een rijtje getallen waar $1, \cdots, 16$ precies een keer in voorkomen. We definiëren $v(S)$ als het aantal paren in S dat verkeerd om staat: het aantal paren getallen (x, y) zodanig dan x in S eerder voorkomt dan y, maar $1 \leq y < x \leq 16$; we geven met $s(S)$ aan het aantal stappen dat $L = 16$ afstaat van de linker-onderhoek. We definiëren $d(S) := v(S) + s(S)$. Verder,

$$\text{als } d(S) \text{ even is dan schrijven we } p(S) = +,$$

$$\text{als } d(S) \text{ oneven is dan schrijven we } p(S) = -;$$

d voor *defect*, en p voor *pariteit*.

Merk op: voor de standaard-situatie S geldt $v(S) = 0$ en $s(S) = 0$ en $p(S) = +$.

(11.4) Een voorbeeld.

L	**14**	**11**	**8**
15	**1**	**5**	**6**
4	**7**	**2**	**3**
12	**10**	**9**	**13**

We zien hier de situatie:

$$L = 16, 14, 11, 8, \quad 15, 1, 5, 6, \quad 4, 7, 2, 3, \quad 12, 10, 9, 13.$$

We geven aan hoeveel cijfers na x kleiner zijn dan x:

$$L = 16\ (15),\ \ 14\ (13),\ \ 11\ (10),\ \ 8\ (7),\quad 15\ (11),\ \ 1\ (0),\ \ 5\ (3),\ \ 6\ (3),$$

$$4\ (2),\ \ 7\ (2),\ \ 2\ (0),\ \ 3\ (0),\quad 12\ (2),\ \ 10\ (1),\ \ 9\ (0),\ \ 13\ (0).$$

We concluderen dat er 69 paren verkeerd om staan: $v(S) = 69$. Het aantal stappen van L tot de linkeronderhoek is $s(S) = 6$. Conclusie: $d(S) = 69 + 6$, en $p(S) = -$.

(11.5) Stelling. *Als we een begin-situatie S hebben m,et $p(S) = -$, dan is deze niet door schuiven in de standaard-situatie over te voeren.* (De puzzel is in de helft van de gevallen niet op te lossen.)

Conclusie. We zien dat deze situatie zoals beschreven in (11.4) door schuiven niet goed te krijgen is (niet over te voeren is in de standaard-situatie).
Gevolg. De opgave gesteld door Sam Loyd, de begin-situatie $1, \cdots, 12, 13, 15, 14, L$, is niet door schuiven tot de standaard-situatie te herleiden: *de puzzel is onoplosbaar.*

Prachtig toch: in plaats van dom en lang proberen, bewijzen we in een paar regels dat de “14-15-puzzel” van Sam Loyd (met de 14 en 15 verwisseld) niet oplosbaar is. Nadenken loont de moeite.

Bewijs van Stelling (11.5). We nemen een situatie S: een rijtje getallen, we schrijven $L = 16$, waar elk van de getallen $1, \cdots, 16$, elk precies een keer in voorkomt. We schrijven S' voor de situatie die we krijgen door precies één keer te schuiven. We bewijzen:

$$p(S) \quad = \quad p(S').$$

Horizontaal schuiven. Als we één keer horizontaal schuiven van verandert $v(S)$ met precies één. Inderdaaad, als we een blokje naar links schuiven, dan gaat $\cdots, L, x, \cdots$ over in $\cdots, x, L, \cdots$ en alle paren ongelijk aan (L, x) blijven in dezelfde stand staan; we zien dat $v(S) - 1 = v(S')$; verder verder verandert $s(S)$ met precies één. We zien dat $d(S) - d(S') \in \{-2, 0, 2\}$. Dus $p(S) \quad = \quad p(S')$ als S' verkregen wordt uit S door precies één keer horizontaal naar links schuiven. Omdat één keer horizontaal naar rechts schuiven $S \mapsto S'$ de omkering is van één keer horizontaal naar links schuiven $S' \mapsto S$, volgt ook voor die handeling $p(S) \quad = \quad p(S')$
Verticaal schuiven. Veronderstel dat we een blokje naar boven schuiven. Dan is S gelijk aan $S = S_1 \cup \{x, y, z, t, L\} \cup S_2$ en $S' = S_1 \cup \{L, y, z, t, x\} \cup S_2$. Bewering: $v(S) - v(S')$ is *oneven*; inderdaad, de paren (x, y), (y, L), en (x, z), (z, L) en (x, t), (t, L) veranderen allemaal en het het paar (x, L) gaat over in (L, x); dit bewijst het gevraagde. Omdat ook $s(S) - s(S')$ oneven is concluderen we $p(S) \quad = \quad p(S')$. Omdat de handeling een blokje naar onderen schuiven de omgekeerde handeling is, volgt ook in die situatie dat $p(S) \quad = \quad p(S')$.

Een eindig aantal keren schuiven is niets anders dan een eindig aantal keren één keer schuiven. We zien dat onder een eindig aantal keren schuiven $p(S)$ niet verandert. Als we beginnen met $p(S) = -$ dan kunnen we niet schuiven tot we in de standaard situatie met $p(\text{standaard}) = +$ komen. Dit bewijst de stelling. QED

(11.6) Omerking. Als $p(S) = +$, dan is deze situatie door schuiven wel over te voeren in de standaard-situatie. Zie (11.14).

(11.7) Conclusie. Van alle begin-situaties is precies de helft on-oplosbaar, en de andere helft oplosbaar.

(11.8) Een voorbeeld bij het bewijs.

•	•	•	•
•	**L**	**7**	**8**
9	**6**	•	•
•	•	•	•

Noem deze situatie S en schuif het blokje 6 naar boven; noem die nieuwe situatie S'. Ga na: $d(S') - d(S) = 7 - 1 = 6$.

(11.9) Opgave. We krijgen het spel, maar nu met letters op de blokjes. Hieronder een begin-situatie. Kunnen we zo schuiven dat de spelling correct wordt?

D	**E**	**N**	**K**
O	**F**	**S**	**C**
H	**U**	**I**	**F**
W	**T**	**A**	

(11.10) We geven nu een behandeling van deze puzzel met een wiskundige methode: *groepentheorie*.

Neem een positief geheel getal n. Een permutatie van de getallen $1, 2, \cdots, n$ is een bijectieve afbeelding

$$\sigma : \quad \{1, 2, \cdots, n\} \quad \longrightarrow \quad \{1, 2, \cdots, n\}.$$

De verzameling van alle permutaties van de getallen $1, 2, \cdots, n$ noteren we met S_n; spreek uit: de *symmetrische groep* op n symbolen. Zie deze handeling als een toevoeging die aan elk getal weer een getal toevoegt.

Opgave.

$$\#(S_n) = n! := 1 \times 2 \times \cdots \times n.$$

Een voorbeeld. Neem $1 \leq i < j \leq N$; definiëer σ als de verwisseling van i en j (en alle andere getallen blijven op de plaats). Deze verwisseling zullen we noteren als $\sigma = (ij)$).

Merk op dat twee permutaties achter elkaar kunnen worden uitgevoerd (compositie):

$$\{1, 2, \cdots, n\} \quad \xrightarrow{\tau} \quad \{1, 2, \cdots, n\} \quad \xrightarrow{\sigma} \quad \{1, 2, \cdots, n\}.$$

Let wel, de handeling $\sigma{\cdot}\tau$ is "eerst τ toepassen, en dan σ toepassen":

$$\sigma{\cdot}\tau(a) \quad = \quad \sigma(\tau(a)).$$

Merk op. Voor elke $\sigma \in S_n$ is er een eenduidige σ^{-1} met: $\sigma{\cdot}\sigma^{-1} = id = \sigma^{-1}{\cdot}\sigma$ (de "inverse); hier is id de identieke afbeelding (alles blijft op zijn plaats). Voor alle σ, τ, φ geldt $\varphi{\cdot}(\tau{\cdot}\sigma) = (\varphi{\cdot}\tau){\cdot}\sigma$. We zien dat we definities van een groep hebben.

Opgave. Elke permutatie kan geschreven worden als een product van verwisselingen.
Pas op. Een dergelijke schrijfwijze is niet eenduidig zoals blijkt uit de volgende opgave: Laat zien dat in S_3 geldt: $(12)(23) = (12)(31)$ (reken het effect uit van de linkerkant en van de rechterkant op elk van de getallen $1, 2$ en 3.
Laat zien dat $(13)(12)(25)(12) = (15)(35)$ in S_5.
Maak zelf nog meer voorbeelden.
Is dit verwarrend? Ja, misschien wel, net zoals al dat schuiven in de puzzel haast niet te volgen is. Hier ontwikkelen we een aparaat om daar systeem in te brengen.

(11.11) Stelling. Laat $\tau_1, \cdots, \tau_s, \sigma_1, \cdots, \sigma_t \in S_n$ verwisselingen zijn zodanig dat

$$\tau_1 \cdot \quad \cdots \quad \cdot \tau_s = \sigma_1 \cdot \quad \cdots \cdot \quad \sigma_t; \quad \text{dan is} \quad s \equiv t \pmod 2.$$

Definitie. We zeggen dat $\varphi \in S_n$ een *even permutatie* is als er een schrijfwijze is

$$\varphi = \tau_1 \cdot \quad \cdots \quad \cdot \tau_s, \text{ waar } \tau_i \text{ verwisselingen zijn, met } s \text{ even,}$$

respectievelijk φ heet oneven als s oneven is.
Opmerking. Omdat de pariteiten van s en t gelijk zijn, volgens de stelling, is deze definitie niet afhankelijk van de gekozenschrijfwijze als product van verwissselingen.
Opgave. Het aantal even permuaties in S_n is gelijk aan $(n!)/2$.

(11.12) Opgave. Zij $\sigma \in S_{16}$, en schrijf op $\sigma(1), \cdots, \sigma(15), \sigma(16)$. In (11.3) hebben we $v(S)$ gedefiniëerd. Laat zien dat $v(S)$ dezelfde pariteit heeft als σ.
Een aanwijzing. Verwissel in deze rij twee getallen als ze "verkeerd om staan', en ga door tot ze allemaal goed staan. Merk opp dat je dat precies even vaak moet doen als het aantal paren dat verkeerd om staat.

(11.13) We geven opnieuw een bewijs van (11.5). Stel $p(S)$ is oneven. Een keer schuiven vermenigvuldigt de permutatie met een verwisseling en verandert $v(S)$ met één. Dus geldt $p(S) = p(S')$. Na een eindig aantal keren schuiven hebben we nog steeds een situatie met pariteit $-$. Conclusie: S kan niet door schuiven opgelost worden. QED

(11.14) We schetseneen oplossing van (11.6). *Als $p(S) = +$ dan kunnen we inerdaad met direct proberen de situatie oplossen.* Het is niet moeilijk, en iedereen die met de 15-puzzel gewerkt heeft weet hoe dit gaat.

Een wiskundig bewijs vinden we in [95]. Zie ook de verwijzingen in dat artikel. Hier is een aanwijzing: Voor elk 3-tal blokjes A, B, C kun je deze cyclisch verwisselen $A \mapsto B, B \mapsto C, C \mapsto A$ (door een serie van handelingen) terwijl de andere tenslotte op hun plaats blijven; inderdaad: schuif alle 3 naar b.v. de linker bovenhoek, handeling α, zodat ze een vierkantje vormen met de lege; dan kun je deze cyclische permutatie uitvoeren, en daarna schuiven we alles weer terug met α^{-1}. Als we steeds beginnen met de lege plek zeg rechts-onder, dan kunnen we al deze cyclische permuaties van drie elementen uitvoeren. Wiskundige stelling: *de 3-cyclische permuaties brengen de groep A_{15} voort*; hier is A_{15} de groep van alle permuaties met $v(S)$ even. Dus kunnen we alles op zijn plaats krijgen. QED

12 Appendix C: RSA

Wiskunde is als zuurstof. Als het er is, merk je het niet.
Als het er niet zou zijn, merk je dat je niet zonder kan.
Lex Schrijver, zie [60], pagina 31.

(12.1) Dit hoofdstuk gaat over *coderingstheorie*. U maakt daar veel gebruik van. Elke keer dat U geld pint wordt de boodschap versleuteld naar de bank gestuurd. Zo kan die boodschap niet ontcijferd worden door mensen die de sleutel niet kennen.

De opgave van coderingstheorie: vind een methode die een bericht versleutelt (en liefst op een manier die publiekelijk bekend is), maar zo dat het ontcijferen (als je een geheim mechanisme niet kent) moeilijk is.

U zult zeggen: als je kunt versleutelen (eindig veel symbolen) dan hoef je toch alleen maar alle mogelijkheden op te schrijven, en terug te zoeken als je wilt ontcijferen. Ja, dat klopt. Maar het is de vraag of dit practisch uitvoerbaar is. Als ik U een dik telefoonboek geef, dan is het gemakkelijk om bij een gegeven naam het bijbehorende telefoonnummer te vinden. Maar, omgekeerd, bij een gegeven telefoonnummer de naam vinden is een enorme klus. Op dit principe berust de RSA publieke-sleutelcrytografie.

In het prachtige boek van Simon Singh hierover vindt U een mooie beschrijving van allerlei coderings-methoden uit het verleden, en ook een beschrijving van RSA, zie [87], §6 en Aanhangsel J. De afkorting RSA staat voor: Ron Rivest - Adi Shamir - Leonard Adleman, de bedenkers van deze cryptografie.

(12.2) Beschrijving van RSA.
Geheim: $p, \ q, \ d,$
Openbaar: $N, \ e.$
Een bericht bestaat uit getallen v met $0 \leq v < N$.
Het versleutelde bericht bestaat ook uit getallen w met $0 \leq w < N$.

Hier geldt: de getallen p en q zijn priemgetallen en $N := p{\cdot}q$; verder is $1 < e < N$ met $\text{ggd}(e, (p-1)(q-1)) = 1$ en $1 < d < N$ met $ed \equiv 1 \pmod{(p-1)(q-1)}$.
Verseutelen: $w = \varphi(v)$; voor gegeven v is w bepaald door $w \equiv v^e \pmod{N}$.
Decoderen: $v = \psi(w)$; voor gegeven w is v bepaald door $v \equiv w^d \pmod{N}$.

Omdat N en e openbaar zijn kan versleutelen van een bericht door iedereen gedaan worden. U zult tegenwerpen dat het bepalen van w met de gewenste eigenschappen een hele klus is (in de praktijk is N een heel groot getal); daar heeft U gelijk in, als je het met de hand zou moeten doen, maar met de moderne computer-techniek is dit een fluitje van een cent.

We zullen zien dat φ en ψ bijectieve afbeeldingen zijn van $W = \{0, 1, \cdots, N-1\}$ naar zichzelf, die bovendien elkaars inverse zijn. We zien dat

$$\varphi : W \xrightarrow{\sim} W \quad \text{de afbeelding} \quad \varphi^{-1} = \psi : W \to W$$

eenduidig vastlegt. Met andere woorden, $\psi(\varphi(v)) = v \quad \forall v \in W$: het ontcijferde bericht komt overeen met het oorspronkelijke.

Hoe valt deze code te breken? Bedenk wel dat N heel groot is (denk aan een getal van 400 cijfers). Daarom is de weg:
[φ helemaal uitschrijven, en in dat "telefoonboek"
voor elke w de ontcijferde $\psi(w)$ opzoeken]
practisch niet uitvoerbaar.

Maar als we d zouden weten, dan kunnen we ontcijferen. In de praktijk blijkt dat we voor het vinden van d met de gewenste eigenschappen de factorizatie $N = p{\cdot}q$ in priemfactoren p en q moeten kennen. Hier zit de bottle-neck: het factoriseren van grote getallen is een enorme klus. Het uitproberen van alle factoren $\leq \sqrt{N}$ is practisch onuitvoerbaar. Er zijn algoritmen om getallen de factorizeren. En nu komt er de wedloop: de code is veilig als N niet gefactoriseerd kan worden; zodra de methoden daartoe efficiënter worden, en de rekenmachines sneller, dan past men de codering aan: grotere p en q (die je moet produceren of kopen).

We leggen uit wat de wiskunde is achter deze cryptografie.

Voor $M \in \mathbb{Z}_{>0}$ schrijven we $\mathbb{Z}/M$ voor de verzameling

$$\mathbb{Z}/M = \{\overline{0}, \overline{1}, \cdots \overline{i}, \cdots, \overline{N-1}\}.$$

Dit is een eindige verzameling. Bovendien kunnen we in deze verzameling "optellen", "aftrekken" en "vermenigvuldigen": we voeren deze handelingen uit alsof we in $\mathbb{Z}$ zijn, en reduceren dan weer modulo M.
Voorbeeld: $M = 7$,; dan is $\overline{5} + \overline{4} = \overline{2}$, omdat $5 + 4 = 2 + 7$ en $\overline{2} \times \overline{4} = \overline{1}$, omdat $2 \times 4 = 1 + 7$.

(12.3) Lemma (de Chinese reststelling). *Onderstel gegeven $m, n \in \mathbb{Z}_{>0}$ met* $\mathrm{ggd}(m, n) = 1$*; schrijf $N = m{\cdot}n$. De natuurlijke afbeelding*

$$\mathbb{Z}/N \quad \xrightarrow{\sim} \quad (\mathbb{Z}/m) \times (\mathbb{Z}/n)$$

is bijectief.
Opmerking: Dit is ook een afbeelding die verwisselt met $+$ en met $\times$: het is een "homomorfisme".

(12.4) Lemma. *Neem de gegevens als in* RSA*. De afbeelding*

$$\varphi : \mathbb{Z}/N \longrightarrow \mathbb{Z}/N, \quad \textit{gegeven door} \quad w \equiv v^e \pmod{N}$$

is bijectief. Uit $ed \equiv 1 \pmod{(p-1)(q-1)}$ *volgt* $\psi{\cdot}\varphi = \mathrm{Id}$.

(12.5) Feit. * *Zij p een priemgetal. Beschouw $(\mathbb{Z}/p)^*$, de multiplicatieve groep van eenheden in $\mathbb{Z}/p$. Merk op: $(\mathbb{Z}/p)^* = \{\overline{1}, \cdots, \overline{p-1}\}$. Beschouw $\mathbb{Z}/(p-1)$ met de optelling als structuur; dit is een groep. Er is een isomorfisme van groepen*

$$\mathbb{Z}/(p-1) \quad \xrightarrow{\sim} \quad (\mathbb{Z}/p)^*.$$

Voorbeelden

$$\mathbb{Z}/6 \longrightarrow (\mathbb{Z}/7)^*, \quad i \bmod 6 \mapsto 3^i \bmod 7,$$

en

$$\mathbb{Z}/96 \longrightarrow (\mathbb{Z}/97)^*, \quad i \bmod 96 \mapsto 2^i \bmod 97,$$

zijn isomorfismen.

Suggestie: schrijf het eerste isomorfisme uit voor alle elementen.

(12.6) Opgave. * Bewijs deze lemma's.

We zien dat de gedachte, en de wiskunde achter der RSA-cryptografie verbluffend eenvoudig is.

13 Appendix D: Enkele notaties en symbolen

Wiskundigen gebruiken sommige notaties en symbolen. Die zijn bedoeld als stenografie. Ze geven een snelle en preciese manier om informatie compact weer te geven. Ik zal me in deze cursus van een paar aspecten van wiskundige notatie bedienen. Het stroomlijnt tekst en uitleg en het maakt wiskundige beweringen vaak nauwkeuriger.

Hieronder geef ik wat notatie. Maar ik geef niet een college logica of verzamelingen-leer.

(13.1) Het esti-symbool. *We schrijven:* $x \in V$*; uit de notatie volgt dat* V *een verzameling is, dat* x *een element is, en dat het element* x *in de verzameling* V *zit.*
Bij voorbeeld, x is de persoon Anne Frank, V is de verzameling van mensen die in de 20ste eeuw geboren zijn; we zien dat $x \in V$ een uitspraak is die waar is, en die we kunnen lezen als: "Anne Frank is in de 20ste eeuw geboren".

We gebruiken het symbool $\notin$ om aan te geven dat het element links ervan niet bevat is in de verzameling rechts daarvan. Zij y de persoon Johann Sebastian Bach. De uitspraak $y \in V$ is niet waar, en $y \notin V$ is wel waar.

(13.2) Inclusie. We gebruiken het symbool $\subset$ om aan te geven dat er links daarvan een verzameling staat, die bevat is in de verzameling die er rechts van staat. Bij voorbeeld laat W de verzameling van Nederlanders zijn geboren in de 20ste eeuw. De uitspraak $W \subset V$, met V als hierboven, is een ware uitspraak.
Pas op. De uitspraak $x \subset V$ is grammaticaal onjuist: het element x wat links staat is niet een verzameling.

(13.3) We geven met $\{\cdots\}$ een verzameling aan, waar tussen te haken gepreciseerd wordt welke elementen beschouwd worden.
Voorbeeld: $\{x\} \subset V$ is een uitspraak equivalent met $x \in V$.
$\{2, 5\} \subset \{1, 2, 3, 4, 5, 6\}$ is een uitspraak die juist is.

(13.4) Gehele getallen. Met $\{z \mid \cdots\}$ geven we aan de verzameling van alle elementen z die voldoen aan de restricties rechts van $|$.
Voorbeeld: met $\{n \mid n \text{ is een geheel getal}\}$ geven we aan de verzameling van alle gehele getallen. Die verzameling zullen we noteren als $\mathbb{Z}$.
$\frac{2}{7} \notin \mathbb{Z}$ en $0 \in \mathbb{Z}$ zijn juist, en $\{-3, 5, 18\} \subset \mathbb{Z}$ is juist.

(13.5) Rationale getallen. De verzameling van *breuken van gehele getallen* geven we aan met $\mathbb{Q}$. Een dergelijk getal wordt een *rationaal* getal genoemd. Merk op dat bij voorbeeld de regel $2/7 = (3{\cdot}2)/(3{\cdot}7)$ geldt. Merk op dat $\mathbb{Z} \subset \mathbb{Q}$; inderdaad een geheel getal $n \in \mathbb{Z}$ kan ook gezien worden als breuk $n/1 \in \mathbb{Q}$.

(13.6) *Er zijn getallen die niet rationaal zijn.*
Bewering. $\sqrt{2} \notin \mathbb{Q}$.
Bewijs. (Bewijs uit het ongerijmde.) Veronderstel dat er gehele getallen $m, n \in \mathbb{Z}$ zijn zodanig dat $\sqrt{2} = m/n$. Kwadrateren geeft: $m^2 = 2{\cdot}n^2$. We weten dat ontbinden van

gehele getallen in priemfactoren uniek is. Het aantal factoren 2 in m^2 is *even*. Het aantal factoren 2 in n^2 is *oneven*. Dit is een tegenspraak. Dit bewijst de bewering. QED

Opmerking. In de oude Griekse wiskunde was dit een schok: dat er getallen bestaan die niet rationaal zijn. Gehele getallen en quotiënten daarvan werden gezien als bouwstenen. Dat er ook andere getallen bestaan werd eerst niet vermoed, en later in de Griekse wiskunde als vreemd ervaren.

We kunnen nog en algemener getal-begrip invoeren. Dit kunnen we doen door bij voorbeeld de verzameling van alle decimale breuken te beschouwen, waar we oneindig veel decimalen achter de komma toelaten. Een dergelijk getal wordt *een reëel getal genoemd*. De verzameling van reële getalen wordt aangegeven met $\mathbb{R}$. We schrijven $\mathbb{C}$ voor de verzameling van complexe getallen: alle getallen van de vorm $a + b\sqrt{-1}$ met $a, b \in \mathbb{R}$. Merk op $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

(13.7) Opmerking. Getallen die beschreven kunnen worden als oplossing van een polynoom-vergelijking worden *algebraïsche getallen* genoemd. Gebruikmakend van het begrip *aftelbaarheid*, zie (13.11)worden aangetoond dat de verzameling van algebraïsche getallen *aftelbaar* is. Omdat het diagonaal-principe van Cantor aantoont dat $\mathbb{R}$ niet aftelbaar is concluderen we: *er zijn reële getallen die niet algebraïsch zijn.* Dit bewijs construeert niet zulke getallen. Het is doorgaans niet zo gemakkelijk constructief het bestaan van zulke getallen aan te tonen.
Voorbeeld. Het getal π is *niet een rationaal getal*, d.w.z. $\pi \notin \mathbb{Q}$ (Lambert 1761; Legendre 1794; Hermite 1873). Pas veel later werd bewezen dat π niet een algebraïsch getal is (Lindemann 1882). Dit resultaat loste een eeuwen-oud probleem op, de kwadratuur van de cirkel: *het is niet mogelijk met passer en liniaal een vierkant te construeren waarvan de oppervlakte gelijk is aan die van een gegeven cirkel.*

(13.8) We geven met $\Rightarrow$ een logische implicatie aan. Bij voorbeeld $x = 1 \Rightarrow x > 0$ is grammaticaal juist en bovendien een ware uitspraak.

Met $\Longleftrightarrow$ geven we een equivalentie van beweringen aan. Met $\wedge$ geven "en" aan en met $\vee$ het zwakke "of". Voorbeelden: $x^2 = 1 \Rightarrow x \leq +1 \vee x \geq -1$.

Het symbool $\cap$ wordt gebruikt voor de doorsnede van verzamelingen (de verzameling van gemeenschappelijke elementen), en met $\cup$ geven we de vereniging aan (de verzameling van elementen die in een van beide ligt, of in allebei).
Voorbeelden: $\{x \mid x \in \mathbb{Z},\quad x \geq 0\} \cap \{x \mid x \in \mathbb{Z},\quad x \leq 0\} = \{0\}$,
$\{x \mid x \in \mathbb{Z},\quad x \geq 0\} \cup \{x \mid x \in \mathbb{Z},\quad x \leq 7\} = \mathbb{Z}$.

(13.9) Met $f : V \to W$ geven we aan dat V en W verzamelingen zijn, en dat f een afbeelding is van V naar W; dat betekent dat f aan elk element van v een element van W toevoegt.

Bij voorbeeld $f : \mathbb{R} \to \mathbb{R}$ gedefiniëerd door $f(x) = x^2$. Dit kan ook weergegeven worden door $x \mapsto x^2$. Let op, de notatie $x \to V$, waar x een element is, is grammaticaal onjuist (aan beiden kanten van $\to$ moet een verzameling staan); de notatie $\{x\} \to V$ is grammaticaal wel juist.

We zeggen dat f *injectief* is als voor alle $v, v' \in V$ geldt $v \neq v' \Rightarrow f(v) \neq f(v')$; schrijfwijze: $f : V \hookrightarrow W$. We kunnen in dit geval V als deelverzameling $f(V)$ van W zien. Voorbeeld: $\mathbb{Z} \hookrightarrow \mathbb{Q}$ door $n \mapsto n/1$.

We zeggen dat $f : V \to W$ *surjectief* als elk element in W het beeld is van een element in V; notatie $f : V \twoheadrightarrow W$. Dit heet ook wel "een afbeeldig van V op W.

Ga na: $f : \mathbb{R} \to \mathbb{R}$ gedefiniëerd door $f(x) = x^2$ is niet injectief, en is niet surjectief.

We schrijven $A \xrightarrow{\sim} B$, en zeggen dit is en *isomorfisme*, als dit een afbeelding is die bijectief is (injectief + surjectief) en bovendien alle structuur links overvoert in die structuur rechts. Voor verzamelingen: bijectief. Voor groepen: + en 0 gaan bovendien in idem over. Voor ringen en lichamen: +, 0, 1 en $\times$ gaan bovendien in idem over. Een isomosfime zegt dat het object links en het object rechts "eigenlijk hetzelfde zijn".

(13.10) $\exists$: er betaat/er bestaan; $\forall$: voor alle.

Met $x := 3$ bedoelen we: "we definiëren x als gelijk te zijn aan 3". Bij het symbool $:=$ staat links een nog niet gedefiniëerd begrip, en rechts ervan iets wat we al kennen.

Met $a \equiv b \pmod{c}$, spreek uit "a is equivalent met b modulo c", bedoelen we: het verschil $a - b$ is deelbaar door c.
Voorbeeld: $1 \equiv 7 \pmod{3}$ is een juiste uitspraak. Ook $2 \not\equiv 7 \pmod{3}$ is juist.
De volgende uitspraak is juist: $a \equiv 0 \pmod{2} \Longleftrightarrow (a$ is even).

Voor een eindige verzameling V schrijven we $\#(V)$ voor het aantal elementen van die verzameling.

Veronderstel dat $a_1, \cdots, a_n$ getallen zijn. De som daarvan wordt genoteerd als

$$\sum_{1 \leq i \leq n} a_i := a_1 + \cdots + a_n; \text{ook wel:} \sum_{i=1}^{i=n}.$$

De notatie $\#(V)$ wordt gebruikt voor het aantal elementen van de verzameling V.

(13.11) We zeggen dat een verzameling *aftelbaar oneindig* is als alle elementen daarvan genummerd kunnen worden met behulp van de positieve gehele getallen $1, 2, 3, \cdots$.

Voorbeeld/Opgave: $\mathbb{Q}$ is aftelbaar oneindig.
Aanwijzing. Laat zien dat het voldoende is om dit te bewijzen voor alle $a/b \in \mathbb{Q}$ met $0 \leq a/b < 1$; zet al die getallen in een (aftelbare) lijst, bij voorbeeld als volgt: $0, 1/2, 1/3, 2/3, 1/4, 3/4, 1/5, 2/5, \cdots$.]

Cantor bewees dat $\mathbb{R}$ niet aftelbaar is. Bij voorbeeld zie
http://en.wikipedia.org/wiki/Cantor's_diagonal_argument

Stelling (Cantor). *De verzameling* $\mathbb{R}$ *is overaftelbaar.*

Dit wil zeggen: als $\alpha_1, \alpha_2, \alpha_3, \dots$ een rij reële getallen is, dan bestaat er een $\beta \notin \mathbb{R}$.
Bewijs. Het is al voldoende om te bewijzen dat de verzameling $\{\gamma \in \mathbb{R} \mid 0 \le \gamma < 1\}$ overaftelbaar is. Veronderstel een dergelijk rij als boven is gegeven met bovendien $0 \le \alpha_i < 1$ voor alle i. Van elk van deze getallen schrijven we de decimale ontwikkeling uit:

$$\alpha_1 = 0,\ a_{1,1}\ a_{1,2}\ a_{1,3}\ a_{1,4} \cdots,$$

$$\alpha_2 = 0,\ a_{2,1}\ a_{2,2}\ a_{2,3}\ a_{2,4}\ \cdots,$$

$$\alpha_3 = 0,\ a_{3,1}\ a_{3,2}\ a_{3,3}\ a_{3,4}\ \cdots,$$

etc.. We construeren positieve gehele getallen $b_1, b_2, \cdots \in \{0, 1\}$ zo dat $b_1 \neq a_{1,1}$, $b_2 \neq a_{2,2}, \quad \cdots b_i \neq a_{i,i}$ voor alle i, b.v. door: als $a_{i,i} > 0$ dan kiezen we $b_i = 0$ en als $a_{i,i} = 0$ dan kiezen we $b_i = 1$. (Dit heet het "Diagonalverfahren".) Schrijf

$$\beta := 0,\ b_1\ b_2\ b_3 \cdots.$$

Omdat $b_i \neq a_{i,i}$ volgt $\beta \neq \alpha_i$ voor elke i; dus komt β niet in bovenstaande lijst voor. We hebben bewezen dat $\mathbb{R}$ overaftelbaar is. QED

Merk op dat decimale schrijfwijze niet uniek is. Het getal $1.\not{9} = 1.999 \cdots$ is gelijk aan twee. Ga na dat dit niet roet in het eten gooit in het bewijs hierboven.

Bewezen kan worden dat alle getallen die voldoen aan een polynoomvergelijking met coëfficienten in $\mathbb{Q}$ een aftelbare verzameling vormt (kunt U dat bewijzen ?). Hieruit volgt dat er transcendente getallen bestaan (getallen die wel in $\mathbb{R}$ gelegen zijn, maar niet vodoen aan een dergelijke polynoomvergelijking. (Zo wordt dat bestaan bewezen zonder dat er een enkel transcendent getal geconstrueerd is.)

(13.12) Samenvatting
$x \in V$ het element x is bevat in de verzameling V; $y \notin V$;
$W \subset V$ deelverzameling; $V \cap W$ doorsnede; $V \cup W$ vereniging;
$\{z \mid \cdots\}$ verzameling van elementen die aan de voorwaarde(n) $\cdots$ voldoen;
$\mathbb{Z}$ verzameling van gehele getallen, $\mathbb{Q}$ van rationale getallen,
$\mathbb{R}$ van reële getallen, $\mathbb{C}$ van complexe getallen;
$f : V \to W$ afbeelding tussen verzamelingen; $\hookrightarrow$ injectief; $\twoheadrightarrow$ surjectief;
$\Longrightarrow$ logische implicatie; $\Longleftrightarrow$ logische equivalentie;
$:=$ links wordt gedefiniëerd door middel van wat er rechts staat;
$a \equiv b \pmod{c}$ "a is equivalent met b modulo c";
$\hookrightarrow$ injectieve afbeelding; $\twoheadrightarrow$ surjectieve afbeelding; $\xrightarrow{\sim}$ een isomorfise;
$\#$ aantal elementen.

14 Appendix E: Enkele wiskundigen

http://en.wikipedia.org/wiki/Timeline_of_mathematics#1s_millennium_BC
http://nl.wikipedia.org/wiki/Lijst_van_wiskundigen
http://www-history.mcs.st-and.ac.uk/history/BiogIndex.html

Pythagoras (Pythagoras van Samos),
geboren tussen 580 en 572 vChr. – gestorven tussen 500 vCHr. en 490 vChr.

Aristoteles (Griekenland, 384 v. Chr. – 322 v. Chr.)

Euclides van Alexandrië (Ptolemaïsch Egypte, circa 365 v. Chr. – 275 v. Chr.)

Archimedes, (Archimedes van Syracuse), (Syracuse, 287 v. Chr. – 212 v. Chr.)

Diophantus, Diophantus van Alexandrië,
(Ptolemaisch Egypte, geboren tussen 200 and 214 – gestorven tussen 284 en 298)

Diophantus van Alexandria (Ptolemaïsch Egypte, circa 298 v. Chr. – 214 v. Chr.)

Abu Ja'far Muhammad ibn Musa Al-Khwarizmi (Irak, geboren ± 780 – gestorven ±850)

Abu Jafar Muhammad ibn al-Hasan Al-Khazin (Iran, ± 900 – ± 971)

Abu Mahmud Hamid ibn al-Khidr Al-Khujandi (Perzië, ± 940 – 1000)

Abu Ali al-Husain ibn Abdallah ibn Sina (Avicenna) (Uzbekistan, 980 – 1037)

Leonardo di Pisa, Leonardo Pisano Fibonacci, of gewoon Fibonacci,
(Italië, geboren tussen 1170 en 1180 - gestorven 1250)

Nicolaus Copernicus (Polen, 1473 – 1543)

Simon Stevin (Nederland, 1548 – 1620)

Johannes Kepler (Duitsland, 1571 – 1630)

Marin Mersenne (Frankrijk, 1588 – 1648)

René Descartes (Frankrijk, 1596 — 1650)

Claude Gaspar Bachet de Mziriac (Frankrijk, 1581 – 1638)

Pierre de Fermat (Frankrijk, 1601 – 1665)

Christiaan Huygens (Nederland, 1629 – 1695)

Isaac Newton (Groot-Brittannië, 1643 – 1727)

Gottfried Wilhelm von Leibniz (Duisland, 1646 – 1716)

Daniel Bernoulli (Zwitserland, 1700 – 1782),
Jakob Bernoulli (Zwitserland, 1654 – 1705),
Johann Bernoulli (Zwitserland, 1667 – 1748),
Nikolaus I Bernoulli (Zwitserland, 1687 – 1759)

Christian Goldbach (Duitsland, 1690 – 1764)

Leonhard Euler (Zwitserland, Rusland, 1707 – 1783)

Johann Heinrich Lambert (Duitsland/Zwitserland, 1728 – 1777)

Joseph-Louis Lagrange (Frankrijk, 1736 – 1813)

Adrien-Marie Legendre (Frankrijk, 1752 – 1833)

Marie-Sophie Germain (Frankrijk, 1776 – 1831) ("Monsieur LeBlanc")

"In describing the honourable mission I charged him with, M. Pernety informed me that he made my name known to you. This leads me to confess that I am not as completely unknown to you as you might believe, but that fearing the ridicule attached to a female scientist, I have previously taken the name of M. LeBlanc in communicating to you those notes that, no doubt, do not deserve the indulgence with which you have responded. Letter to Gauss (1807)" Zie ook de Nederlandse versie van [86], pag. 129.

Carl Friedrich Gauss (Duitsland, 1777 – 1855)

Jean Victor Poncelet (Frankrijk, 1788 - 1867)

Augustin Louis Cauchy (Frankrijk, 1789 – 1857)

August Ferdinand Mbius (Duitsland, 1790 – 1868)

Niels Henrik Abel (Noorwegen, 1801 – 1829)

Johann Peter Gustav Lejeune Dirichlet (Duitsland, 1805 – 1859)

Ernst Eduard Kummer (Duitsland, 1810 – 1893)

Eugne Charles Catalan (België, 1814 – 1894)

Pierre Laurent Wantzel (Frankrijk, 1814 – 1848)

Karl Weierstrass (Duitsland, 1815 – 1897)

Evariste Galois (Frankrijk, 1811 – 1832)

Pafnuty Lvovich Chebyshev (Rusland, 1821 – 1894)

Bernhard Riemann (Duitsland, 1826 – 1866)

Franz Mertens (Duitsland, 1840-1927)

Max Noether (Duitsland, 1844 – 1921)

Georg Ferdinand Cantor (Duitsland, 1845 – 1918)

Felix Klein (Duitsland, 1849 – 1925)

Sofia Vasilyevna Kovalevskaya (Rusland, 1850 – 1891)

Carl Louis Ferdinand von Lindemann (Duitsland, 1852 – 1939)

Hendrik Lorentz (Nederland, 1853 – 1928)

Henri Poincaré (Frankrijk, 1854 – 1912)

Thomas Jan Stieltjes (Nederland, 1856 – 1894)

David Hilbert (Duitsland, 1862 – 1943)

Jacques Salomon Hadamard (Frankrijk, 1865 - 1963)

Charles-Jean de La Valle Poussin (België, 1866 - 1962)

Luitzen Egbertus Jan Brouwer (Nederland, 1881 – 1966)

Emmy Noether (Duitsland, 1882-1935)

Viggo Brun (Noorwegen, 1885-1978)

Hermann Weyl (Duitsland, USA, 1885-1955)

György Pólya (Hongarije, 1887 – 1985)

Srinivasa Aiyangar Ramanujan (India, Groot-Brittannië, 1887 – 1920)

Dirk Jan Struik (Nederland, USA, 1894 – 2000)

Maurits Cornelius Escher (Nederlands kunstenaar 1898 – 1972)

Oscar Zariski (Wit-Rusland, USA, 1899 – 1986)

William Vallance Douglas Hodge (Schotland, 1903 – 1975)

Bartel Leendert van der Waerden (Nederland, 1903 – 1996)

Hans Freudenthal (Duitsland, Nederland 1905 – 1990)

Andre Weil (Frankrijk, 1906 – 1998)

Alan Mathison Turing (Groot-Brittannië, 1912 – 1954)

Paul Erdös (Polen, 1913 – 1996)

Atle Selberg (Noorwegen, 1917-2007)

Richard Phillips Feynman (USA, 1918 – 1988)

Kurt Gödel (Duitsland, 1906 – 1978)

Jean-Pierre Serre (Frankrijk, 1926–)

Yutaka Taniyama (Japan, 1927 – 1958)

Alexander Grothendieck (Duitsland, Frankrijk 1928 –)

Goro Shimura (Japan, 1930 –)

Roger Penrose (Groot-Brittannië, 1931 –)

Robert Phelan Langlands (, Canada, USA, 1936 –)

Barry Charles Mazur (USA, 1937 –)

David Bryant Mumford (Groot-Brittannië, USA 1937 –)

Don Berhard Zagier (U.S.A., Duitsland, 1951 –)

Yoichi Miyaoka (Japan)

Victor Kolyvagin (Rusland)

Matthias Flach (USA)

Andrew Wiles (Groot-Brittannië, 1953 –)

Gerd Faltings (Duitsland, 1954 –)

Kenneth Alan (Ken) Ribet (USA)

Richard Taylor (Groot-Brittannië, USA, 1962 –)

Grigori Perelman (Rusland, 1966 –)

15 Appendix F: Groepen, ringen en lichamen*

In de tekst komen we de begrippen “groep” en “ring” tegen. in deze appendix geven we de precieze definities. Voor het volgen van de hoofdlijn van de cursus zijn deze begrippen niet nodig. Voor het begrijpen van een paar technische details zijn deze eenvoudige algebraïsche begrippen nuttig. Elk boek over abstracte algebra bevat deze definities. B.v. zie [55].

(15.1) Definitie. Een *groep* G is een (niet-lege) verzameling met de volgende eigenschappen: er is een element $e \in G$ (het eenheidselement, er is een afbeelding $* : G \times G \to G$ (de vermenigvuldiging, of compositie, of optelling) en een afbeelding $i : G \to G$ (de inverse) zodanig dat:

$$(a * (b * c)) = ((a * b) * c) \quad a * i(a) = e = i(a) * a, \qquad \forall a, b, c \in G.$$

We zeggen dat G commutatief is als $a * b = b * a, \quad \forall a, b.$

Groepen komen heel veel voor “in de natuur”. De unificerende werking van deze definitie heeft een enorme invloed gehad op de ontwikkeling van de wiskunde.

(15.2) Voorbeeld. $G = \mathbb{Z}$, met $* = +$, en $i(n) = -n$.

(15.3) Voorbeeld. Zij X een meetkundige figuur met bepaalde eigenschappen (afmetingen, of een andere structuur). Zij G de verzameling van isomorfismen $\varphi : X \xrightarrow{\sim} X$ (een bijectieve afbeelding, die alle structuur behoudt). De identieke afbeelding noemen we e. We schrijven $\psi * \varphi = \psi \cdot \varphi$ voor de compositie: achter elkaar uitvoeren; let wel, we hebben het gebruik om te defniéren $\psi \cdot \varphi(x) = \psi(\varphi(x))$, m.a.w. eerst φ uitvoeren, en dan pas ψ uitvoeren.

(15.4) Voorbeeld. Zij $X = \{1, \cdots n\}$. Zij $G = S_n$ de verzameling van bijectieve afbeeldingen $\varphi : X \to X$ (dat heet een permutatie). Met compositie vormt dit een groep. Er zijn $n!$ elementen in G, waar $n! := 1 \times 2 \times \cdots \times n$.
Opgave. Ga na: als $n > 2$, dan is S_n niet-commutatief.

(15.5) Andere voorbeelden:
(1) $\mathbb{Z}/n$: neem $\{0, 1, \cdots, n-1\}$ met “optellen modulo n” als groepswet;
(2) $\{+1, -1\}$ met $\times$ als $\times$ groepswet; ga na dat $\{+1, -1\}$ (multiplicatief) en $\mathbb{Z}/2$ (additief) isomorf zijn (dat wil zegen we beelde de ene bijectief op de andere af zodat de groepswetten in elkaar overgaan);
(3) zij p een priemgetal; neem $\{1, 2, \cdots, p-1\}$, multiplicatief; we schrijven dit als $(\mathbb{Z}/p)^*$; bewezen kan worden dat $\mathbb{Z}/(p-1)$ additief en $(\mathbb{Z}/p)^*$ isomorf zijn; dit wordt ook wel verwoord als: $(\mathbb{Z}/p)^*$ is “cyclisch”.

(15.6) Definitie. Een *ring* R is een (niet-lege) verameling met de volgende eigenschappen: er zijn elementen $0 \in R$, $1 \in R$, er is een afbeelding $\times : R \times R \to R$ (de vermenigvuldiging, soms genoteerd als $a \cdot b$), er is een afbeelding $+ : R \times R \to R$ (de optelling) die *commutatief* verondersteld wordt, en er is een afbeelding $- : R \to R$ (de inverse voor de optelling) zodanig dat $(R, o, +, -)$ een groep is, en zodanig dat

$$a\cdot(b\cdot c) = (a\cdot b)\cdot c, \quad (a+b)\cdot c = a\cdot c + b\cdot c \quad c\cdot(a+b) = c\cdot a + c\cdot b \qquad \forall a,b,c \in R.$$

(15.7) Voorbeeld. $R = \mathbb{Z}$ met de gebruikelijke operaties; $R = \mathbb{Z}[\sqrt{-3}]$.

(15.8) Opmerking. We komen vaak ringen tegen waar bovendien de vermenigvuldiging commutatief is. Maar er zijn ook (heel interssante) ringen waar welikswaar (per defintie) de optelling commutatief is, maar de vermenigvuldiging niet commutatief ia.

Voor iemnad die weet wat matrices zijn: neem alle 2×2 matrices met elementen uit $\mathbb{Z}$. Optellen van matrices is optellen van de getallen in de matrices die op dezelfde plaats staan. Vermenigvuldigen is vermenigvulidgen van matrices. Zo komt er een ring, die men wel noteert als $\mathrm{Mat}(2, \mathbb{Z})$. Laat zien dat voor elke matrix waarvan de diagonaal elementen niet gelijk zijn, er een matrix is die er niet mee commuteert.

(15.9) Definitie. Een *lichaam* is een ring K waarin de vermenigvuldiging commutatief is, met $0 \neq 1$, en bovendien is er een operatie$()^{-1} : K \to K$ gegeven zodanig dat $(K - \{0\}, 1, \times)$ een commutatieve groep is.

Met andere woorden een ring is een lichaam, $K \neq \{0\}$, waar de vermenigvuldiging commutatief is en elke element ongelijk aan nul een inverse heeft.

(15.10) Voorbeelden. $K = \mathbb{Q}$, $\quad K = \mathbb{R}$, $\quad K = \mathbb{Z}/p$, waar p een priemgetal is. Ga na: $\mathbb{Z}$ is niet een lichaam.

(15.11) Voorbeeld. Beschouw de verzameling K bestaande uit alle getallen (elementen van $\mathbb{R}$) van de vorm $a + b\sqrt{2}$. Optellen en vermenigvulidgen zoals in $\mathbb{R}$.
(1) Laat zien dat dit een lichaam geeft; dit wordt genoteerd als $K = \mathbb{Q}(\sqrt{2})$.
(2) Laat zien dat de bovenstande schrijfwijze uniek is; dat wil zeggen: als $a, b, c, d \in \mathbb{Q}$ met $a + b\sqrt{2} = c + d\sqrt{2}$ dan geldt $a = c$ en $b = d$. In dit geval beschouwen we K als een "vectorruimte van dimensie 2 over $\mathbb{Q}$".We komen hier nog uitvoerig op terug in het college.

16 Appendix G: Ontbinden in factoren

Hier vermelden we een paar feiten die we in de tekst gebruiken.

(16.1) Definitie. We werken in de verzameling $\mathbb{Z}$ van alle gehele getallen. De notatie $d \mid a$ wordt gebruikt voor: d deelt a; dat wil zeggen, er betaat een b met $d{\cdot}b = a$. we zeggen ook wel: D is een deler van a.
Een getal $p \in \mathbb{Z}_{>1}$ heet een *priemgetal* als 1 en p de enige positieve delers van p zijn:

$$d \in \mathbb{Z}_{>1}, \quad d \mid p \quad \Longrightarrow \quad d = p.$$

(16.2) Opmerking. Elk getal $a \in \mathbb{Z}_{>1}$ is deelbaar door een priemgetal.
Bewijs. Merk op dat de bewering juist is voor $a = 2$. Neem aan dat de bewering juist is voor alle a' met $1 < a' < a$ (inductie-aanname). Als a een priemgetal is dan zijn we klaar. Als A niet een priemgetal is, dan heeft a een deler d heeft met $1 < d < a$. Schrijf $a = d{\cdot}a'$. De inductie veronderstelling bewijst dat er een priemgetal p is dat a' deelt. Dan is p ook een deler van a. QED

(16.3) Stelling. *Voor elk getal $a \in \mathbb{Z}_{>1}$ is er een ontbinding $a = p_1 \times \cdots \times p_t$ in priemfactoren. Bovendien is deze schrijfwijze uniek op volgorde na.*
Hiermee wordt bedoeld: voor elke $n \in \mathbb{Z}$ met $n \notin \{-1, 0, +1\}$ bestaan er priemgetallen $p_1, \cdots, p_s$ met $n = \pm p_1 \times \cdots \times p_s$. Bovendien als $p_1 \times \cdots \times p_s = \ell_1 \times \cdots \times \ell_t$ waar alle factoren priemgetallen zijn, dan is $s = t$ en na eventueel omnummeren geldt $p_1 = \ell_1, \ \cdots \ , p_s = \ell_s$.

We hoeven alleen maar factorizatie voor positieve gehele getallen te beschouwen. We kunnen (formeel) ook staande houden dat 1 een dergelijk factorizatie heeft, door te postuleren dat het lege product de waarde 1 heeft.

We ontwikkelen een methode om dit te bewijzen.

(16.4) Opmerking. Vroeger, bv. in de tijd van Euler werd ook $a = 1$ als priemgetal gezien. Nu hebben we een iets andere definitie, die $a = 1$ uitsluit als priemgetal.

(16.5) Waarschuwing. We zijn zo gewend dat "ontbinding in irreducibele factoren" eenduidig is op eenheden en volgorde na. In $\mathbb{Z}$ geldt dat op $\pm$ na: $6 = 2{\cdot}3 = (-2){\cdot}(-3)$. In het algemeen geldt die eenduidigheid in een willekeurige ring niet. Hier is een voorbeeld: neem de ring

$$T := \mathbb{Z}[\sqrt{-5}] = \{x + y{\cdot}\alpha \mid x, y \in \mathbb{Z}\},$$

met $\alpha^2 = -5$, bij voorbeeld als deelverzameling van $\mathbb{C}$ beschouwd. Merk op dat in T geldt:

$$2{\cdot}3 \quad = \quad 6 \quad = \quad (1 + \sqrt{-5}){\cdot}(1 - \sqrt{-5});$$

Het is gemakkelijk in te zien dat de factoren $2, 3, (1 + \sqrt{-5}), (1 - \sqrt{-5}) \in T$ irreducibel zijn. Ook zien we dat $+1, -1 \in T$ de eenheden zijn. Hier zien we dat er niet sprake is van eenduidige factorontbinding in déze ring T.

Voor we aan een bewijs beginnen gaan we eerst een fundamenteel hulpmiddel invoeren: de *eenduidigheid van factorizatie* in $\mathbb{Z}$.

Merk op dat als voor gehele getallen $d, e \in \mathbb{Z}$ geldt $d{\cdot}e = 1$ dan is óf $e = +1$ óf $e = -1$. We zullen $+1$ en -1 de eenheden van $\mathbb{Z}$ noemen. De enige positieve delers van een priemgetal p zijn 1 en p zelf. Als we schrijven $n = \pm p_1 \times \cdots \times p_s$, waar $p_1, \cdots, p_s$ priemgetallen zijn, dan spreken we van een (priem)factorizatie van het gehele getal n.

(16.6) Lemma (deling met rest). *Laat gegeven zijn gehele getallen $n, d \in \mathbb{Z}$ met $d > 0$. Dan bestaan er $q, r \in \mathbb{Z}$ zodanig dat:*

$$n = q{\cdot}d + r \quad \textit{met} \quad 0 \leq r < d.$$

Bewijs. Voor elke $j \in \mathbb{Z}$ beschouw

$$I_j = \{jd, jd+1, \cdots jd+d-1\} = \{m \in \mathbb{Z} \mid jd \leq m < (j+1)d\}.$$

Duidelijk: $j \neq k$ dan is $I_j \cap I_k = \emptyset$ en

$$\mathbb{Z} = \cdots \cup I_{-1} \cup I_0 \cup I_1 \cup I_2 \cup \cdots \ .$$

Hieruit volgt dat er voor elke $n \in \mathbb{Z}$ er precies één $q \in \mathbb{Z}$ is met $n \in I_q$. Dit is equivalent met $n = q{\cdot}d + r$ met $0 \leq r < d$. QED

(16.7) De grootste gemene deler. We zeggen dat $d \in \mathbb{Z}$ een *deler* is van $a \in \mathbb{Z}$ als er bestaat een $d' \in \mathbb{Z}$ zodanig dat $d{\cdot}d' = a$. We noteren dit als $d \mid a$; als c niet een deler is van a dan noteren we dit als $c \not| \, a$.
Voor $a \in \mathbb{Z}$ definiëren we $\mid a \mid$, de absolute waarde van a als volgt: als $a \geq 0$ dan is $\mid a \mid = a$; als $a \leq 0$ dan is $\mid a \mid = -a$.
Zij gegeven $a,\ b \in \mathbb{Z}$. We definiëren de grootste gemene deler d van a en b als volgt: beschouw

$$\{\delta \quad | \quad 0 \leq \delta \leq \mid a \mid, \quad 0 \leq \delta \leq \mid b \mid, \quad \delta \text{ deelt } a, \quad \delta \text{ deelt } b\};$$

merk op dat deze verzameling niet leeg is (ga alle mogelijke gevallen na). Het grootste getal in deze verzameling noteren we als $\mathrm{ggd}(a,b)$, de grootste gemene deler $d = \mathrm{ggd}(a,b)$ van a en b. Merk op: voor $a = 0$ geldt $\mathrm{ggd}(0,b) = b$; voor $a \neq 0$ en $b \neq 0$ geldt $\mathrm{ggd}(a,b) > 0$. Als $\mathrm{ggd}(a,b) = 1$, dan zeggen we dat a en b *onderling ondeelbaar* zijn.

(16.8) Lemma. *Zij gegeven $a,\ b \in \mathbb{Z}$. Schrijf $d := \mathrm{ggd}(a,b)$. Er bestaan $x, y \in \mathbb{Z}$ zodanig dat*

$$xa + yb = d.$$

Bewijs. Als $a = 0$ of $b = 0$, dan is de uitspraak waar (ga na). Beschouw alle paren gehele getallen (α, β) zodanig dat $\mid \alpha \mid \geq \mid \beta \mid > 0$ en $\mathrm{ggd}(\alpha, \beta) = d$. Als $\beta = d$ dan kunnen we de gevraagde x en y vinden: $0{\cdot}\alpha + 1{\cdot}\beta = d$. We beschouwen nu $\mid a \mid \geq \mid b \mid > d$ en we nemen aan (inductie hypothese) dat de uitspraak waar is voor alle paren (α, β) als boven met $\mid b \mid > \mid \beta \mid \geq d$. Uit (16.6) volgt dat er bestaat:

$$a = q{\cdot}b + r \quad \text{met} \quad 0 \leq r < \mid b \mid .$$

Ga na: $\text{ggd}(a,b) = \text{ggd}(b,r)$. De inductie hypothese zegt dat we kunnen kiezen $x', y' \in \mathbb{Z}$ met

$$x'{\cdot}b + y'{\cdot}r = d; \quad \text{dus} \quad y'{\cdot}a - q{\cdot}b + x'{\cdot}b = d.$$

Voor $x := y'$ en $y := -q + x'$ krijgen we de gevraagde uitspraak. QED

Een voorbeeld/toepassing. Zij $a = p$ een priemgetal en beschouw $b \in \mathbb{Z}$. Als p een deler is van b dan geldt $\text{ggd}(p,b) = p$. Als p niet een deler is van b dan geldt $\text{ggd}(p,b) = 1$ en er bestaan $x, y \in \mathbb{Z}$ met $xp + yb = 1$.

Bewijs van (16.3). Als n een priemgetal is dan is factorizatie mogelijk (met één priemfactor). Onderstel dat $n > 1$ niet een priemgetal is, en dat factorizatie mogelijk is voor alle m met $1 < m < n$. Omdat n niet een priemgetal is, zijn er echte delers, d.w.z. we kunnen schrijven $a = b{\cdot}b'$ met $1 < b$ en $1 < b'$. Voor b en voor b' is priemfactorizatie mogelijk (de inductie hypothese). Dus volgt factorizatie voor n. Dit bewijst het bestaan van priemfactorizatie voor alle $n \in \mathbb{Z}_{>1}$. Nu nog de eenduidigheid.

Neem aan dat $p_1 \times \cdots \times p_s = \ell_1 \times \cdots \times \ell_t$ met $1 \leq s \leq t$ (anders links en rechts verwisselen). Schrijf $p = p_1$.

Bewering. Er is een index $1 \leq j \leq t$ zodanig dat $p = \ell_j$.

Bewijs. Als dit niet het geval zou zijn, dan zijn er x_i, y_i met $x_i p + y_i \ell_i = 1$ voor alle $1 \leq i \leq t$. Dan zou gelden

$$p{\cdot}(p_2 \times \cdots \times p_s)(y_1 \times \cdots \times y_t) = (1 - x_1 p) \times \cdots \times (1 - x_t p).$$

Dit kunnen we herschrijven als

$$p{\cdot}A = 1 + p{\cdot}B, \qquad A, B \in \mathbb{Z}; \qquad (A - B){\cdot}p = 1.$$

Deze tegenspraak bewijs de bewering.

Kies $s \leq t$ in een factorizatie als boven en neem aan dat eenduidigheid bewezen is in alle gevallen met kleinere s. Uit de aanname volgt dat

$$p_2 \times \cdots \times p_s = \ell_1 \times \cdots \times \ell_{j-1} \times \ell_{j+1} \cdots \times \times \ell_t.$$

Uit de inductie-hypothese volgt dat hier eenduidigheid op volgorde na geldt. Dit bewijst ook die eenduidigheid voor $p_1 \cdots p_s = \ell_1 \cdots \ell_t$. Dit bewijst de eenduidigheid. QED (16.3)

17 Apendix H: Een paar puzzels

(17.1) Betegeling van een gehavende rechthoek. Gegeven zijn $m, n \in \mathbb{Z}_{>0}$, en een rechthoek B van afmeting $m \times n$. Deze rechthoek is door middel van horizontale en vertical lijnen verdeeld in mn vierkanten van afmeting 1×1. Het rechtsonder en het linksboven vierkant worden van B weggehaald, en het resultaat (een gehavende rechthoek) noemen we B'. We hebben voldoende dominostenen van afmeting 2×1. *Kunnen we B' betegelen met zulke dominostenen* ? (die mogen zowel horizontaal als verticaal gelegd worden; geen overlap; heel B' dient belegd te zijn; dominostenen mogen niet doormidden worden gezaagd). Zie

http://www.vierkantvoorwiskunde.nl/puzzels/puzzelmarkt.html E5

(17.2) Verhuizen.
Zie http://www.vierkantvoorwiskunde.nl/puzzels/puzzelmarkt.html F3
Opgave. Er zijn gegeven $m, n \in \mathbb{Z}_{>0}$. Er is een rechthoekig wooncomplex met afmeting $m \times n$ verdeeld in kamers van afmeting 1×1 en ik elke kamer is één persoon. Er zijn voldoende deuren tussen alle kamers. Op een dag besluiten ze allemaal te verhuizen: iedereen gaat naar een kamer daarnaast (maar niet diagonaal). *Voor welke waarden van m en n kan deze verhuizing geschieden zodat daarna er weer in elke kamer is één persoon is ?*

(17.3) Een wandeling door een flat.
Zie http://www.vierkantvoorwiskunde.nl/puzzels/puzzelmarkt.html F4
Opgave. In een kubus-vormig flatgebouw met afmeting $3 \times 3 \times 3$ zijn er kamer van afmeting $1 \times 1 \times 1$. Er zijn deuren tussen twee aangrenzende kamers, en er zijn trappen tussen kamers die pal onder elkaar liggen. Iemand begint in de middelste kamer (de kamer op de middelste verdieping, zonder uitzicht) met een rondwandeling met het doel alle kamers precies één keer te passeren. *Is die rondwandeling mogelijk ?*

Als die persoon in een andere kamer begint hoe beslissen we dan of in dat geval een rondwandeling mogelijk is?

(17.4) Loodlijnen.
Zie: http://www.vierkantvoorwiskunde.nl/puzzels/puzzelmarkt.html F5
In een gelijkzijdige driehoek ABC kiezen we een punt P (in het inwendige of op een van de zijden, of in een hoekpunt). We laten uit P de drie loodlijnen PQ, PR, en PS op de drie zijden neer. *Laat zien dat de som van de lengtes $\mid PQ \mid + \mid PR \mid + \mid PS \mid$ onafhankelijk is van de keuze van het punt P.*

(17.5) Het schudden van handen.
Opgave. Een intelligent persoon S en zijn partner p zijn op een feestje. Daar zijn nog 4 andere paren (dus in totaal $10 = 5 \times 2$ personen). Tijdens het feest schudden sommige mensen elkaar de hand, maar daarbij houden ze zich aan de volgende regels:

a) Niemand schudt de hand met zichzelf.

b) Niemand schudt de hand met de partner.

Aan het eind van het feest vraagt S aan alle andere gasten (inclusief de partner p)

hoeveel verschillende personen elk de hand heeft geschud. Elk van die 9 personen geeft een ander antwoord. Hoeveel mensen heeft S een hand geschud?
Merk op: iedereen schudt hooguit 8 keer met iemand de hand. We zien dus dat de antwoorden zijn: $0, 1, \cdots, 8$.

(17.6) Een getal van 10 cijfers.
Opgave. Welk getal van 10 cijfers voldoet aan de volgende regels:
Het eerste cijfer geeft het aantal nullen (0) in het getal.
Het tweede cijfer geeft het aantal enen (1) in het getal.
Het derde cijfer geeft het aantal tweeën (2) in het getal.
Het vierde cijfer geeft het aantal drieën (3) in het getal.
Het vijfde cijfer geeft het aantal vieren (4) in het getal.
Het zesde cijfer geeft het aantal vijven (5) in het getal.
Het zevende cijfer geeft het aantal zessen (6) in het getal.
Het achtste cijfer geeft het aantal zevens (7) in het getal.
Het negende cijfer geeft het aantal achten (8) in het getal.
Het tiende cijfer geeft het aantal negens (9) in het getal.
Bepaal dit getal.

(17.7) Een product van twee getallen.
Opgave. Bewijs: *Voor elke $s \in \mathbb{Z}_{>0}$ is er een $t \in \mathbb{Z}_{>0}$ zodanig dat $s \times t$ een getal is dat alleen maar uit de cijfers 0 en 7 bestaat.*

(17.8) Niet een kwadraat.
Opgave. *Bewijs dat voor elke $n \in \mathbb{Z}_{>0}$ het getal $2^n + 3^n$ niet het kwadraat is van een geheel getal.*

(17.9) De 3 sollicitanten.
Opgave. Drie sollicitanten lijken even goed, en er komt een laatste test. Er zijn 5 hoeden: 2 zwarte en 3 witte. De spelregels worden uitgelegd. De sollicitanten gaan achter elkaar staan, en krijgen een hoed op. De achterste ziet de twee voorgangers, de middelste zie alleen de voorste, en de voorste ziet niemand. Daarna wordt van achteraf aan gevraagd wat de kleur is van de hoed die ze op hebben.Ze mogen kiezen waar te gaan staan, en
Arend gaat gauw achteraan staan, want hij denkt dat dat de beste plaats is;
Boudewijn neemt dan maar de middelste positie, en
Carlijn gaat vooraan staan, want zij denkt dat dat de beste plaats is.
Ze worden geblinddoekt, elk krijgt een hoed op, de resterende twee hoeden gaan in de kast, kastdeur dicht, en de blinddoeken gaan weer af.

Dan wordt aan Arend gevraagd of hij weet wat de kleur is van zijn hoed; Arend kan het wel raden, maar dat mag niet, en hij weet het niet zeker. Ook Boudewijn weet niet wat de kleur van zijn hoed is. Daarna zegt Carlijn dat ze weet wat de kleur van haar hoed is.
Wat is de kleur van die hoed, en door middel van welke redenering weet Carlijn dat?

In opgave (17.9) zien we dat informatie wat anderen weten soms voldoende kan zijn voor het trekken van een conclusie. We geven daar nog een mooier voorbeeld van in de volgende Opgave (17.10).

(17.10) Gemutste dwergen.
Opgave. Er was eens een volk dwergen. Allemaal erg slim. En ze konden ook heel goed rekenen en tellen. En het volk had een wijze en aardig koning. De koning had een prachtige kroon op, en de overige dwergen hadden elk een muts op, sommige dwergen een rode muts, sommige dwergen een witte. Maar niemand wist wat de kleur van de eigen muts is. En daar werd ook niet over gepraat. Er waren geen spiegels, de mutsen werden nooit afgezet, kortom er was geen enkel middel voor elke dwerg om de kleur van de eigen muts te weten te komen. De koning besloot daar verandering in te brengen.

Hij riep alle dwergen bij elkaar. "Ik zie dat er tenminste één witte en tenminste één rode muts is. Vanavond komen we met z'n allen bij elkaar, en morgenavond weer en zo gaan we door. Als op een avond iemand weet wat de kleur van de eigen muts is dan mag die persoon / die personen bij mij die avond komen eten, en die onderdanen komen dan de volgende avond niet meer naar de bijeenkomst.
Stel dat er 4 rode en 27 witte mutsen zijn. Op welke avonden komen er hoeveel onderdanen eten bij de koning?
Een voorbeeld. Als er één rode muts is, en 33 witte mutsen, dan komt er op de eerste avond één onderdaan eten, en de tweede avond 33 onderdanen. Want: de dwerg met de rode muts ziet alleen maar witte mutsen; de koning zei dat er tenminste een rode muts is; hij heeft dus een rode muts op; de andere dwergen zien één rode muts bij een andere dwergen op de eerste avond; dan zouden ze nog zelf en rode of een witte muts op kunnen hebben. Maar de tweede avond is die rode muts er niet meer; die wist dus dat hij een rode ophad; dat kan alleen maar als er geen andere rode mutsen zijn; de andere dwergen weten op de tweede avond dus dat ze een witte muts ophebben.

Suggestie. Werk eerst het voorbeeld uit waar er precies twee rode mutsen zijn en 38 witte mutsen.

Geef een oplossing van de opgave. Geef vervolgens een oplossing van de opgave met R rode mutsen en W mutsen (let wel $R > 0$ en $W > 0$).

(17.11)
I know an old man in Tralee
Whose age is his wife's age plus three.
Now he rightly declares,
That the sum of their squares
Is a square; so how old could he be?

(17.12) Oplossing van Opgave (17.1).
(a) *Als $m+n$ even is, dan is een betegeling van B' met zulke dominostenen niet mogelijk.*
(b) *Als $m+n$ oneven is, dan is een dergelijke betegeling wel mogelijk.*
Bewijs. Geef de vierkanten van B de kleuren wit en zwart, zodat aangrenzende vierkantjes verschillende kleuren hebben (denk aan een schaakbord).

(a) Als $m + n$ even is dan hebben we van B twee vierkantjes verwijderd van dezelfde kleur. Laat zien dat het aantal W' van witte vierkantjes van B' niet gelijk is aan het aantal Z' van zwarte vierkantjes van B'. Betegeling met dominostenen is dus niet mogelijk in dit geval.
(b) Onderstel dat m oneven is en n even. We kunnen B' verdelen in twee rijen van lengte $m - 1$ (de rijen waar de vierkantjes uit verwijderd zijn), en een rechthoek van afmeting $m \times (n - 2)$. De rijen kunnen betegeld worden met dominostenen die horizontaal gelegd worden. De overblijvende kolommen met dominostenen die verticaal gelegd worden. QED

(17.13) Oplossing van Opgave (17.2). a) Voor m en n oneven is dit niet mogelijk, (b) voor alle andere gevallen is dit wel mogelijk.
Bewijs. Nummer de kamers met indices $1, \cdots, m$ en $1, \cdots, n$.
(b) Als m even is, dan gaat bewoner $B_{i,j}$ met i oneven naar kamer $K_{i+1,j}$ en voor i even gaat $B_{i,j}$ naar $K_{i-1,j}$. Als n even is dan doen we hetzelfde maar met verwisselen via de tweede index.
Conclusie. Als m even of n even (of allebei even) dan is de verhuizing mogelijk.

(a) We bewijzen nu dat verhuizen voor m en n beide oneven niet mogelijk is. Laten we de kamers, net als op een schaakbord, om en om de kleuren wit en zwart geven. Merk op dat in dit geval het aantal zwarte velden niet gelijk is aan het aantal witte velden. Maar bij verhuizen gaat elke bewoner van een zwarte kamer naar een witte, en elke bewoner van een witte kamer naar een zwarte; tegenspraak. (Hier is een keuze voor de kleuren: de kamer $K_{i,j}$ met $i + j$ even krijgt een zwarte kleur, en met $i + j$ oneven krijgt een witte kleur.)

(17.14) Oplossing van Opgave (17.3). (a) Die rondwandeling is niet mogelijk in het geval begonnen wordt in de middelste kamer.
(b) Er zijn 13 start-posities van waaruit de rondwandeling niet mogelijk is, en er zijn 14 startposities van waaruit de rondwandeling wel mogelijk is.
Geef zelf een bewijs. Hint: zie de oplossing van (17.2).

(17.15) Hint bij Opgave (17.4). Trek lijnen door P evenwijdig aan de zijden van de driehoek.

(17.16) Oplossing van Opgave (17.5). Antwoord: S heeft met 4 personen de hand geschud.

We zullen dit bewijzen. Het is eenvoudiger om het in een algemenere vorm te doen:

(17.17) Opgave (17.5)'. Dezelfde opgave voor een feestje met $2N$ (in plaats van 10) personen bestaande uit N paren (in plaats van 5 paren) met $N > 0$. Deze situatie/opgave geven we aan met $\mathcal{O}(N)$.

(17.18) Oplossing en bewijs van Opgave (17.5)'. **Antwoord.** S heeft in de situatie $\mathcal{O}(N)$ met $N-1$ personen de hand geschud.
Bewijs. Eerst een opmerking:

In de opgave met M paren, met $M > 1$, is er een paar (A, a), verschillend van (S, p), met $\#A = 2M - 2$ en $\#a = 0$.

Hier schrijven we $\#x$ voor het aantal keren dat persoon x iemand een hand geschud heeft.
Bewijs van de opmerking. Er is iemand die $2M - 2$ handen geschud heeft. Dat is niet p, want er is ook iemand die helemaal geen handen geschud heeft. Dus is er een A die niet S en die niet p is met $\#A = 2M - 2$. Die heeft alle andere mensen behalve zijn partner de hand geschud; die mensen hebben allemaal de eigenschap $\#x > 0$. Dus heeft a, de partner van A, niemand de hand geschud. Dit bewijst de opmerking.

Bewijs van de oplossing van Opgave (17.5)'.
We doen dit met inductie naar M. Voor $M = 1$ is de uitspraak waar. (Als we dit niet een goed uitgangspunt vinden, dan nemen we $M = 2$ en gebruiken de bovenstaande opmerking.)

Neem aan dat er een $N > 0$ is waarvoor de uitspraak $S(N)$ juist is; we bewijzen dan de uitspraak $\mathcal{O}(N + 1)$.

Uit de opmerking zien we dat er in die verzameling $F(N+1)$ van $N+1$ paren er een paar (A, a) is met $\#A = 2N$ en $\#a = 0$. Verwijder die personen uit de verzameilng $F(N+1)$ en schrap ook alle handen die A gegeven heeft. Dan komen we in de situatie $F(N)$ zoals in $\mathcal{O}(N)$. Daar heeft S met precies $N-1$ personen de hand geschud (inductie-aanname). Dus in de situatie $\mathcal{O}(N + 1)$ heeft S met $N - 1$ personen en met A de hand geschud, in totaal daarom met N personen. Dit bewijst de inductie stap, en een bewijs van opgave (17.5)' is gegeven. QED

(17.19) Opmerking/Opgave. Laat zien dat in de situatie $\mathcal{O}(N)$ het feestje bestaat uit de paren $(S, p), (A_1, a_1), \cdots, (A_{N-1}, a_{N-1})$ met: $\#(S) = N - 1 = \#(p)$ en $\#A_i = 2N - 1 - i$ en $\#a_i = i - 1$ voor $1 \leq i \leq N - 1$.

(17.20) Opgave (17.6): **Oplossing / Bewering.**
Het getal 6210001000 beantwoordt aan de condities.
Bovendien zijn geen andere getallen die voldoen aan de voorwaarden.
Bewijs. Het is duidelijk dat het gegeven getal aan de voorwaarden voldoet. We gaan nu bewijzen dat dit de enige oplossing is.
Schrijf het getal als $a_0 a_1 \cdots a_8 a_9$ met $0 \leq a_i \leq 9$ voor alle i. Dan geldt:

$$\textbf{(1)} \qquad a_0 + a_1 + \cdots + a_8 + a_9 = 10;$$

want dit geeft precies het aantal cijfers aan in het getal.

We geven eerst het bewijs in een bijzonder geval, ter illustratie van het algemene bewijs.

Onderstel dat $a_0 = 7$. We zien dat van de 10 getallen er precies 7 gelijk aan 0 zijn. Behalve a_0 zijn er dan nog twee die ongelijk aan nul zijn. Die twee getallen zijn positief, hun som is $10 - a_0 = 3$. Dus zijn die getallen gelijk aan 1, respectivelijk gelijk aan 2. Maar dat is een tegenspraak, want $a_i = 2$ zou betekenen dat het getal i twee keer voorkomt, wat niet het geval is in $10 = 7 + 2 + 1$. Conclusie: $a_0 \neq 7$.

Merk op dat $a_0 \neq 0$: dat zou een tegenspraak "met zichzelf" geven. We hebben gebruikt de regel:

(2) onder de getallen $a_1, a_2, \cdots a_9$ zijn er precies $10 - a_0 - 1$ ongelijk aan nul, en hun som is gelijk aan $10 - a_0$.

Conclusie. We hebben gezien dat $a_0 > 0$. Gebruik makend van de regels (1) en (2) zien we dat dit geeft $10 = a_0 + 2 + 1 + \cdots + 1$. Als $a_0 = 2$ komt er tegenspraak: in dat geval komt het getal 1 precies 6 voor, maar geen van de getallen is gelijk aan 6. Als $a_0 > 2$ dan is er een getal dat precies 2 keer voorkomt; dat gebeurt alleen als $10 = 6+2+1+1$. Dit bewijst dat dit de enige oplossing is. QED

(17.21) Oplossing van Opgave (17.7).
Notatie/opmerking. We schrijven $G(c)$ voor de verzameling van natuurlijke getallen die alleen maar bestaan uit het cijfer 0 en het cijfer c. We merken op dat als $s \times t' \in G(1)$, dan is $s \times ct' \in G(c)$. we zien dus dat de opgave veel algemener kan: het cijfer 7 kan vervangen worden door een c met $0 < c < 10$, en dat die algemenere opgave opgelost is als we de opgave met $G(1)$ oplossen.
Oplossing van Opgave (17.7) **met** 7 **vervangen door** 1.
Opgave Kies $s \in \mathbb{Z}_{>0}$. Beschouw de verzameling $\{1 \times 10^i \mid i \in \mathbb{Z}_{>0}\}$. Dit is een oneindige verzameling. Beschouw de resten na deling door s. We concluderen:

er is een u met $0 \leq u < s$ en een oneindige verzameling $J \subset \mathbb{Z}_{>0}$ zodanig dat

$$j \in J \Longrightarrow 10^j \equiv u \pmod{s}.$$

Kies

$$j_s < j_{s-1} < \cdots < j_2 < j_1 \quad \text{in} \quad J.$$

Dan is s een deler van

$$\sum_{k=1}^{k=s} 10^{j_k} =: N; \quad \text{schrijf} \quad \frac{N}{s} = t'.$$

Dan is $s \times t' \in G(1)$ en $s \times 7t' \in G(7)$. QED

(17.22) Oplossing van Opgave (17.8). Voor $n \in \mathbb{Z}_{>0}$ geldt

$$2^n + 3^n \equiv (-1)^n \pmod{3}.$$

Omdat -1 niet en $+1$ wel een kwadraat in $\mathbb{Z}/3$ is volgt dat n even is; schrijf $n = 2j$. We zien

$$2^{2j} + 3^{2j} \equiv (-1)^j + (-1)^j \pmod 5.$$

De kwadraten in $\mathbb{Z}/5$ zijn $\{0, 1, 4\}$. Maar

voor j even geldt: $(-1)^j + (-1)^j \equiv 2 \pmod 5$;

voor j oneven geldt: $(-1)^j + (-1)j \equiv -2 \pmod 5$.

Dus is $2^n + 3^n$ niet een kwadraat. QED

(17.23) Oplossing van Opgave (17.9).
Carlijn heeft een witte hoed op.
Het argument:

omdat Arend het niet weet, zijn de voorste twee hoeden niet zwart.

Boudewijn weet het vervolgens niet.

Als Carlijn een zwarte hoed op zou hebben, dan had Boudewijn kunnen concluderen dat de zijne wit is; maar Boudewijn weet het niet. Dus heeft Carlijn een witte hoed op. QED

(17.24) Oplossing van Opgave (17.10). Bij 4 rode mutsen en 33 mutsen komen er op de 4-de avond de dwergen met de rode mutsen eten, en op de 5-de avond komen de andere 33 dwergen bij de koning eten.

Algemener. Met R rode mutsen en W mutsen. Als $R < W$ dan komen er op avond R (en niet eerder) de dwergen met rode musten eten en op avond $R + 1$ (en niet eerder) de dwergen met witte mutsen.
Als $W < R$ dan komen er op avond W de dwergen met rode mutsen eten en op avond $R + 1$ de anderen.
Als $W = R$ dan komen er op avond W alle dwergen bij de koning eten.

(17.25) Bewijs van de oplossing van Opgave (17.10). We geven de oplossing voor het geval $R < W$ (en de andere gevalen gaan net zo). We schrijven $\mathcal{O}(R)$ voor de opgave met R rode mutsen en $W \geq R$ witte mutsen.
Het geval van $\mathcal{O}(1)$ hebben we boven reeds opgelost, en daar is de oplossing zoals in (17.24).
Inductie-aanname. Er is een getal $i \geq 1$ waarvoor we weten oplossing (17.24) juist is in de situatie $\mathcal{O}(j)$ voor elke j met $1 \leq j \leq i$.
Inductie-stap. Onderstel we zijn in de situatie $\mathcal{O}(i + 1)$. Verplaatsen we ons in de gedachten van een dwerg D met een rode muts. Die ziet steeds i rode mutsen.

Maar op een eerdere avonden zijn die dwergen niet gaan eten bij de koning. Uit de inductie veronderstelling volgt: er zijn er in totaal niet i rode mutsen. Na avond i concludeert D dat zijn muts ook rood is. Dit geldt voor alle dwergen met rode mutsen. Alle dwergen met rode mutsen in de situatie $\mathcal{O}(i+1)$ gaan op avond $i+1$ bij de koning eten. Beschouw nu $W > i + 1$; de dwergen met een witte muts zien steeds $i + 1$ rode mutsen; zelf zouden ze een rode of en witte muts op kunnen hebben. Tot en met avond $i + 1$ kunnen ze nog niet beslissen wat die kleur is, en daarom gaan die dwergen niet op avond $i+1$ bij de koning eten. Maar op avond $i+2$ zien ze geen rode mutsen meer. Die dwergen weten dan (inductie-aanname) dat er precies $i+1$ rode mutsen waren, en dat ze daarom zelf een witte ophebben, en ze gaan op avond $i+2$ bij de koning eten.

(17.26) Oplossing van Opgave (17.11).
De man is 63 jaar oud. We zien: $60^2 + 63^2 = 87^2$.
Hoe komen we aan een dergelijke oplossing? We kunnen proberen: laat het getal M de waarden 4 tot 120 doorlopen, en bepaal of $(M-3)^2 + M^2$ een kwadraat is. Dat komt alleen maar voor als $M = 12$, en als $M = 63$ (een nare rekenpartij).

Men kan dit ook als volgt bewijzen bewijzen. Euclides liet zien:
Als $x, y, z \in \mathbb{Z}_{>0}$ *met* $x^2 + y^2 = z^2$ *dan zijn er* $m, n, d \in \mathbb{Z}_{>0}$ *zodanig dat*
$x = d(m^2 - n^2), \quad y = 2dmn, \quad z = d(m^2 = b^2).$

Als we eisen dat bovendien $\mid x - y \mid = 3$ dan zien we:
voor $d = 1$ komt er geen oplossing;

voor $d = 3$ en $n = 1, \quad m = 2$ komt er: $(x = 9, y = 12, z = 15)$;

voor $d = 3$, en $n = 2, \quad m = 5$ komt er $(x = 63, y = 60, z = 87)$;

voor andere $d, \quad n$ en m zijn er nog oplossingen mogelijk, b.v. $(d = 3, n = 5, m = 12)$, $(d = 3, n = 12, m = 19)$ maar alle met $x > 300$, en $y > 300$. Het is onwaarschijnlijk dat een man, zelfs in Tralee, zo oud zou zijn. (Bestaat Tralee wel? ja hoor, een klein plaatsje in Zuidwest Ierland.)

Referenties

[1] Anonymous Arab manuscript (before 972) in the Imperial Library of Paris.
French translation by F. Woepcke: *Recherches sur plusieurs ouvrages de Léonard de Pise.*
III: *Traduction d'un fragment anonyme sur la formations des triangles rectangles en nombres entiers, et d'un traité sur je même sujet par Aboū Dja'far Mohammed Ben Alhoçain.* Vol. **14** pp 211 – 227, 241 – 269, 301 – 324, 343 – 356.
Also published: F. Woepcke - Études sur les mathématiques Arabo-Islamiques. Band II. Nachdruck aus den Jahren 1842 – 1974. Herausgegeben von Fust Sezgin. Inst. Geschichte Arabisch-Islamischen Wissensch., Goethe-Universität, Frankfurt am Main, 1986.

[2] R. Alter – *The congruent number problem.* American Mathematical Monthly **87** (1980), 43 – 45.

[3] T. M. Apostol – *Introduction to analytic number theory.* Undergraduate Texts Math., Springer – Verlag, 1976.

[4] L.Bastien – *Nombres congruents.* Intermédiare des Math. **22** (1915), 231 – 232.

[5] A. H. Beiler - *Recreations in the theory of numbers: The queen of mathematics untertains.* Dover Publ., pocket, 1964.

[6] E. T. Bell – *Men of mathematics.* Simon & Schuster. 1937.

[7] F. Beukers – *Getaltheorie voor beginners.* Epsilon uitgaven, 1999.

[8] B. Birch & H. Swinnerton-Dyer – *Notes on elliptic curves II.* Journal für die reine und angewandte Mathematik **218** (1965), 79-108.

[9] V. Brun – *La serie 1/5+1/7+1/11+1/13+1/17+1/19+1/29+ 1/31+1/41+1/43+1/59+1/61+..., les dénominateurs sont nombres premiers jumeaux est convergente où finie.* Bull. Sci. Math. **43** (1919), 124-128.

[10] L. L. Bucciarelli & N. Dworsky – *Sophie Germain. An essay in the history of the theory of elasticity.* Reidel Publ. Cy, 1980.

[11] W. K. Bühler – *Gauss: A biographical study.* Springer – Verlag, Berlin, 1981.

[12] D. M. Burton - *Elementary number theory.* Allyn & Bacon, 1980.

[13] E. C. Catalan – *Note extraite d'une lettre adressée à l'éditeur.* Journal für die reine und angewandte Mathematik **27** (1844), 192.

[14] V. Chandrasekar – *The congruent number problem.* Resonance August 1998, 33 – 45.
http://www.ias.ac.in/resonance/Aug1998/pdf/Aug1998p33-45.pdf

[15] J. Coates & A. Wiles – *On the conjecture of Birch and Swinnerton-Dyer.* Invent. Math. **39** (1977), 223-251.

[16] J. H. Coates – *Congruent number problem.* Quarterly Journal of pure and Applied Mathematics **1** (2005), 14 – 27.

[17] H. Darmon, F. Diamond & R. Taylor - Fermat's Last Theorem. In: Curr. Developments in Math., 1995. Internat. Press, Harvard Univ.

[18] B. Datta & A. N. Singh – *History of Hindu mathematics.* Asia Publ. House, Part I: 1935, Part II: 1938, Single volume edition: 1962.

[19] M. Davis, Yu. Matijesevic and J. Robinson – *Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution.* Proceed. Sympos. Pure Math **28** (1976), AMS Part 2, pp. 323 – 378.

[20] L. E. Dickson – *History of the theory of numbers.* Volume II: Diophantine analysis. Chelsea publ. Cy. New York, 1952. .

[21] U. Dudley – *History of formula for primes.* American Mathematical Monthly **76** (1969), 23 – 28.

[22] U. Dudley – *Formulas for primes.* Math. Magazine, **56** (1983), 17 – 22.

[23] G. W. Dunnington – *Carl Friedrich Gauss: Titan of Science.* Hafner Publ. Co. 1955 (The Mathematical Association of America, June 2003).

[24] G. W. Dunnington – *The Sesquicentennial of the Birth of Gauss.* Scientific Monthly, XXIV (May, 1927): 402 – 414. Zie:

http://www.mathsong.com/cfgauss/Dunnington/1927

[25] A. Doxiadis – *Oom Petros en het vermoeden van Goldbach.* De Bezige Bij, 2000. Voor een bespreking van dit boek zie:
http://www.math.leidenuniv.nl/ naw/serie5/deel02/mrt2001/pdf/goldbach.pdf

[26] H. M. Edwards – *Riemann's zeta function.* Academic Press, 1974. Herdrukt: Dover Publications, 2001.

[27] H. M. Edwards – *Fermat's last theorem. A genetic introduction to algebraic number theory.* Grad. Texts Math. 50, Springer – Verlag, 1977.

[28] N. D. Elkies – *Curves* $Dy^2 = x^3 - x$ *of odd analytic rank.* Proceedings of ANTS-5, 2002 (C.Fieker and D.R.Kohel, eds.), Lecture Notes in Computer Science 2369, pp. 244-251.

[29] *Leonhard Euler und Christian Goldbach, Briefwechsel, 1729 - 1764.* Editors A. P. Juškevič & E. Winter. Berlin, Akademie-Verlag, 1965.

[30] G. Frey - Links between solutions of A-B=C and elliptic curves. In: Number theory, Ulm 1987 (Ed. H. P. Schlickewei & E. Wirsing). Lect. N. Math. 1380, Springer - Verlag 1989, pp. 31-62.

[31] A. Fröhlich & M. J. Taylor - Algebraic number theory. Cambridge Std. Advanc. Math. 27, Cambridge Univ. Press, 1991.

[32] Leonardo Pisano Fibonacci – *The book of squares.* An annotated translation into modern English by L. E Sigler. Academic Press 1987.

[33] D. Fowler & E Robson – *Square root approximations in old Babylonian mathematics.* YBC 7289 in context, Historia Math. **25** (1998), 366-378.

[34] M. Gardner - *Mathematical games.* Scientific American, 1977, 101 – 121.

[35] M. Gardner – *The Colossal Book of Mathematics.* W. W. Norton & Co 2001. Chapter 7: "Penrose Tiles".

[36] C. F. Gauss – *Disquisitiones Arithmeticae,* 1798, gepublicerd in Leipzig, 1801.
Er zijn veel vertalingen. B.v.:
(vertaald door Arthur A. Clarke) – *Disquisitiones Aritmeticae.* Yale University Press, 1965.

[37] G. Giorello & C. Sinigaglia – *Fermat. De meester van de moderne mathematica.* NWT, Veen Magazines, 2006; ISBN: 9076988889.
Oorspronkelijk titel: "Fermat - i sogni di un magistro all'origine della matematica moderna."

[38] C. Goldstein, N. Schappacher & J.Schwermer – *The shaping of arithmetic after C. F. Gausss Disquisitiones Arithmeticae.* Springer Berlin Heidelberg, 2007.

[39] J. Gray – *The Hilbert challenge.* Oxford University Press, 2000.

[40] M. W. Gray – *Sophie Germain.* In: Complexities in mathematics (Eds B. A. Case, A. M. Leggett), Princeton University Press, 2005; pp. 64 – 74.

[41] R. K. Guy – *Unsolved problems in number theory.* Springer – Verlag, 3rd Edition 2004.

[42] T. Hall – *Carl Frederich Gauss: a biography.* Cambridge, MA: MIT Press. 1970.

[43] G. H. Hardy & E. M. Wright - *An introduction to the theory of numbers.* Oxford, Clarendon Press, fourth edition, 1975.

[44] T. Heath – *A history of Greek mathematics.* Oxford, Clarendon Press, 1921.

[45] Y. Hellegouarch – *Invitation to the mathematics of Fermat-Wiles.* Academic Press, 2002.

[46] *Briefwechsel zwischen Alexander von Humboldt und Carl Friedrich Gauss.* Editor: K.-R Biermann. Berlin : Akademie-Verlag, 1977.

[47] J. P. Jones, D. Sato, H. Wada & D. Wiens – *Diophantine representations of prime numbers.* Amer. math. Monthly **83** (1976), 449 - 464.

[48] D. Kehlmann – *Die Vermessung der Welt.* Roman. Rowohlt Verlag, Reinbek 2005. Er is ook een Nedelandse ("Het meten van de wereld") en een Engelse vertaling ("Measuring the world") van dit boek.

[49] A. W. Knapp – *Elliptic curves.* Math. Notes 40, Princeton Univ. Press, 1992.

[50] A. N. Kolmogorov & A P. Yushkevich – *Mathematics of the 19th century.* Birkhäuser, 1992.

[51] N. Koblitz – *Introduction to elliptic curves and modular forms.* Grad. Texts Math. 97, Springer - Verlag, 1984.

[52] G. Kramarz – *All congruent numbers less than 2000.* Math. Ann. **273** (1986), 337 – 340.

[53] S. Lang – *Die abc-Vermutung.* El. Math. 48 (1993), 89 - 99.

[54] S. Lang – *Algebraic number theory.* Grad. Texts Math. 110, Springer Verlag, 1986.

[55] S. Lang – *Algebra.* Addison - Wesley Publ. Cy, 1965.

[56] A.-M. Legendre – *Essai sur la théorie des nombres.* Paris, 1798. Latere druk: *Théorie des nombres.*

[57] B. Mazur – *Number theory as a gadfly.* Amer. Math. Monthly 98 (1991), 593-610.

[58] U. C. Merzbach – *Carl Friedrich Gauss: a bibliography.* Scholarly Resources Inc. Wilmington Delaware, 1984.

[59] P. Mihăilescu – *Primary cyclotomic units and a proof of Catalan's conjecture.* Journal für die reine und angewandte Mathematik **572** (2004), 167195.

[60] B. Mols – *Opgelost. Toepassingen van wiskunde en informatica.* Veen Magazines, 2006; ISBN: 10-9085710286

[61] P. Monsky – *Mock Heegner points and congruent numbers.* Math. Zeitschrift **204** (1990), 45-67.

[62] J. Moser – *A prime representing this function.* Math. Magazine **23** (1950), 163-164.

[63] D. Musielak – *Sophie's diary.* AuthorHouse, 2008.

http://www.amazon.com/gp/reader/1418408123/ref=sib_dp_pt# reader-link

[64] J. Oesterlé - Nouvelles approaches du "théorème"de Fermat. Sém. Bourbaki **40** (1987/88), Exp. 694. Astérisque 161-162 (1988), 165-186.

[65] F. Oort — *Priemgetallen.* In: Kaleidoscoop van de wiskunde 1. Editors: F. van der Blij, J. P. Hogendijk, F. Oort. Epsilon Uitgaven, 1990; pp.1 – 32.

[66] F. Oort – *Congruent numbers in the tenth and in the twentieth century.* In: Vrolijk, Arnoud & Jan P. Hogendijk (eds.), O ye Gentlemen: Arabic Studies on Science and Literary Culture, in Honour of Remke Kruk. - Leiden [etc.]: Brill, 2007.

[67] F. Oort – *Congruente getallen.* Syllabus Kaleidoscooop van de wiskunde, 10-II-2009. Zie:

http://www.math.uu.nl/people/oort/

[68] E. P. Ozhigova – *C. F. Gauss, Übersicht über die Gründe der Constructibilität des Siebzehneckes.* Istoriko-mat. Issledovaniya 21, 1976

[69] E. Picutti – *Sui numeri congruo-congruenti di Leonardo Pisano.* Physis **23** (1981), 141 – 170.

[70] K. Plofker – *Mathematics in India.* Princeton University Press, 2008.

[71] A. de Polignac – *Recherches nouvelles sur les nombres premiers.* Comptes Rendus des Séances de l'Académie des Sciences, 1849.

[72] P. Ribenboim – *13 lectures on Fermat's last theorem.* Springer - Verlag, 1979.

[73] P. Ribenboim – *The new book of prime number records.* Springer – Verlag, 1996.

[74] K. A. Ribet – *From the Taniyama-Shimura conjecture to Fermat's last theorem.* Ann. Fac. Sc. Univ. Toulouse 11 (1990), 116-139.

[75] K. Ribet – *Wiles proves Taniyama's conjecture; Fermat's last theorem follows.* Notices A.M.S. **40** (1993), 575-576.

[76] B Riemann – *Über die Anzahl der Primzahlen unter einer gegebenen Grösze.* Monatsberichte der Berliner Akademie (1859).
Zie http://www.claymath.org/millennium/Riemann_Hypothesis/1859_manuscript/

[77] H. Riesel - *Prime numbers and computer methods for factorization.* Progress Math. 57, Birkhäuser, 1985.

[78] K. H. Rosen – *Elementary number theory and its applications.* Addison Wesley, 2000.

[79] B. Rosser – *Explicit bounds for some functions of prime numbers.* American Journal of Mathematics **63** (1941), 211232.

[80] E. S. Rowland – *A natural prime-generating recurrence.* Journal of Integer Sequences, **11** (2008), Article 08.2.8.

[81] M. du Sautoy – *The music of the primes.* Harper Collins, 2003.

[82] J-P. Serre - Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbb{Q}}/\mathbb{Q}$). Duke Math. Journ. **54**, (1987), 179-230.

[83] J. Sesiano – *Books IV to VII of Diophantus' Arithmetica.* Sources Hist. Math. Phys. Sciences **3**. Springer – Verlag 1982.

[84] D. Shanks - *Solved and unsolved problems in number theory.* Chelsea Publ. Cy., 1978.

[85] J. H. Silverman – *The arithmetic of elliptic curves.* Grad. Texts Math. 106, Springer -Verlag, 1986.

[86] S. Singh – *Fermats Last Theorem.* Fourth Estate, 1997.
Vertaald in het Nederlands:
S. Singh – *Het Laatste raadsel van Fermat.* Arbeiderspers, 1998.

[87] S. Singh – *The code book, the science of secrecy from ancient Egypt to quantum cryptography.* , Fourth Estate, 1999.
S. Singh – *Code, de wedloop tussenmakers en brekers van geheime codes en cijferschrift.* De Arbeiderspers, 1999.
http://www.math.leidenuniv.nl/ naw/serie5/deel01/jun2000/pdf/vermeulen.pdf

[88] S. Singh – *Big bang: the origin of the universe.* Fourth Estate, 2004.
http://www.simonsingh.net/Big_Bang_Reviews.html
S. Singh – *De oerknal.* De Arbeiderspers, 2005

[89] B. de Smit, J. Top e.a. – *Speeltuin van de wiskunde.* Veen Magazines, NWT, 2003.
ISBN: 907698820X paperback

[90] N. M. Stephens – *Congruence properties of congruent numbers.* Bull. London Math. Soc. **7** (1975), 182-184.

[91] "*De laatste stelling van Fermat*", Syllabus van lezingen gehouden op 6-XI-1993. WG & Universiteit Utrecht.

[92] R. Tijdeman – *On the equation of Catalan.* Acta Arithmetica **29** (1976), 197-209

[93] J. B. Tunnell – *A classical diophantine problem and modular forms.* Invent. Math. **72** (1983), 323 - 334.

[94] W. T. Tuttle – *Graph theory.* Encyclop. Math. Applications, Vol 21, Addison-Wesley Publ. Cy, 1984.

[95] W. Waalewijn – *Schuifpuzzels.* Nieuw Archief voor Wiskunde, Serie 5, Nummer **4.3** (september 20(1837)03), 240 – 241.

[96] M. L. Wantzel – *Recherches sur les moyens de reconnaître si un Problème de Géométrie peut se résoudre avec la règle et le compas.* Journal de Mathématiques Pures et Appliquées 1 (2) (1837), 366372.
(M. staat voor Monsieur; de voornamen van Wantzel zijn Pierre Laurent.)

[97] A. Weil – *Number theory, an approach through history, from Hammurapi to Legendre.* Birkhäuser 1984.

[98] E. Weiss – *Algebraic number theory.* Mc-Graw-Hill Cy, 1963.

[99] A. Wiles – *Modular elliptic curves and Fermat's Last Theorem.* Annals Math. **141** (1995), 443 – 551.

[100] D. Zagier – *Die ersten 50 Million Primzahlen.* Zeitschrift Elemente der Mathematik, Beiheft Nr 15, Birkhäuser Verlag, 1977; 14 pp.
Ook: *The first 50 million prime numbers.* The Math. Intelligencer, **0** (1977), 7 – 19.

http://modular.math.washington.edu/edu/2007/simuw07/misc/zagier-the_first_50_million_prime_numbers.pdf

Prof. Dr F. Oort
Mathematisch Instituut
P.O. Box. 80.010
NL - 3508 TA Utrecht
The Netherlands
email: oort@math.uu.nl